



JPCERT/CC 四半期レポート

2026 年 7 月 1 日～2026 年 9 月 30 日

2026 年 10 月 22 日



サイバーインシデントがなくなるその日まで。

JPCERT Coordination Center

一般社団法人 JPCERT コーディネーションセンター

はじめに

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）は、インターネット利用組織におけるコンピューターセキュリティインシデント（以下「インシデント」）の認知と対処およびインシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として国内外の関係機関と調整活動を行っています。

これらの活動のほとんどを、「令和 8 年度サイバー攻撃等国際連携対応調整事業」（経済産業省委託事業）および「令和 8 年度サイバー対処能力の強化に向けたインシデント情報等に関する周知等の事務」（内閣官房委託事業）として実施しています。

本レポートでは、2026 年 7 月 1 日～2026 年 9 月 30 日 までの活動について報告しています。

なお、「第 4 章 国内連携活動」「第 5 章 国際連携活動」「第 6 章 フィッシング対策協議会活動」「第 7 章 広報活動」には、受託事業以外の自主活動に関する記載が一部含まれています。

2026 年 10 月 1 日、JPCERT/CC は創立 30 周年の節目を迎えました。活動を支えてくださる皆さまに御礼申し上げます。

目次

はじめに	1
トピックス&ハイライト	5
JPCERT/CC 創立 30 周年	5
第 1 章 インシデント対応支援および脅威情報分析	9
1.1 インシデント対応支援	9
1.1.1 四半期の統計情報	9
1.1.2 インシデントの傾向	15
1.1.2.1 フィッシングサイトの傾向	15
1.1.2.2 Web サイト改ざんの傾向	16
正規 Web サイトに海外オンラインカジノサイトなどのリンクが大量に埋め込まれた事例	16
外部から取得したコードを実行する JavaScript が EC サイトに埋め込まれた事例	17
1.1.2.3 標的型攻撃の傾向	17
マルウェア LotusLite への感染を狙った標的型攻撃メール	17
1.1.2.4 その他のインシデントの傾向	17
1.2 脅威情報の分析と提供	17
1.2.1 情報収集・分析	18
1.2.2 Web サイトでの情報提供	18
1.2.2.1 注意喚起	18
1.2.2.2 CyberNewsFlash	19
1.2.2.3 Weekly Report	20
1.2.3 CISTA での情報提供	20
1.2.3.1 早期警戒情報	20
1.2.3.2 Analyst Note	20
1.2.3.3 インディケーター情報	21
1.2.3.4 個別提供情報	21
1.2.4 対応事例	21
1.2.4.1 多数の FortiGate の設定から窃取し収集されたとみられる大量の FortiGate 管理者の認証情報	21
1.2.4.2 Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性 (CVE-2026-66066)	23
1.2.4.3 NetScaler ADC および NetScaler Gateway におけるメモリバッファオーバーランの脆弱性 (CVE-2026-8452)	23
第 2 章 インターネット上の探索活動や攻撃活動に関する観測と分析	25

2.1	インターネット定点観測システム「TSUBAME」を用いた観測	25
2.1.1	TSUBAME 観測動向	25
2.1.2	TSUBAME の観測データの活用	27
2.2	ハニーポットの運用とその分析	27
2.2.1	AI / LLM 開発者ツールを狙う攻撃活動の観測	27
2.2.2	IoT 機器を標的としたボットネットによるスキャン活動	28
第 3 章	脆弱性関連情報の調整と流通	30
3.1	脆弱性関連情報の取り扱い状況	30
3.1.1	JPCERT/CC における脆弱性関連情報の取り扱い	30
3.1.2	Japan Vulnerability Notes (JVN) において公表した脆弱性情報および対応状況	31
3.1.2.1	特筆すべきパートナーシップガイドラインに基づき報告された脆弱性	32
	JVN#40688603 miChecker における XML 外部実体参照 (XXE) に関する脆弱性	32
3.1.2.2	特筆すべき国際調整または独自調整で取り扱った脆弱性	32
	JVNVU#95422936 古野電気製 FA-50 (簡易型船舶自動識別装置、AIS) におけるハードコードされた認証情報使用および認証欠如の脆弱性	32
3.1.3	連絡不能開発者対応	33
3.1.4	CNA および Root としての活動	33
3.2	日本国内の脆弱性情報流通体制の整備	34
3.2.1	日本国内製品開発者との連携	34
3.2.2	製品開発者との定期ミーティング等の実施	34
第 4 章	国内連携活動	36
4.1	業界団体やコミュニティ等との連携活動	36
4.1.1	日本貿易会 ISAC	36
4.1.2	SICE/JEITA/JEMIMA セキュリティ調査研究合同ワーキンググループ	36
4.1.3	セプターカウンシル運営委員会	36
4.2	国内関係機関との連携強化および情報交換の環境整備	37
4.2.1	CISTA 利用組織との連携促進	37
4.2.2	製造業の制御システムセキュリティ担当者向け課題検討グループ	37
4.3	情報・ツール等の提供	37
4.3.1	制御システム向けセキュリティ自己評価ツールの提供	37
第 5 章	国際連携活動	38
5.1	海外 CSIRT 構築支援および運用支援活動	38
5.2	国際 CSIRT 間連携	38
5.2.1	APCERT (Asia Pacific Computer Emergency Response Team)	38
5.2.1.1	APCERT Steering Committee 会議の実施	39
5.2.1.2	APCERT サイバー演習 (APCERT Drill) 2026 への参加	39
5.2.2	FIRST (Forum of Incident Response and Security Teams)	39
5.3	海外 CSIRT 等の来訪および訪問	39
5.4	その他国際会議への参加	40
5.4.1	APNIC 62 に参加・登壇	40
5.5	国際標準化活動	40

5.6	脆弱性調整および情報流通に関する国際的な協力体制の構築	40
第 6 章	フィッシング対策協議会活動	41
6.1	フィッシング対策協議会事務局の運営	41
6.1.1	フィッシングに関する報告・問い合わせの受け付け	41
6.1.2	情報収集／配信	43
6.1.2.1	定期報告	43
6.1.2.2	フィッシングサイト URL 情報の提供	43
6.1.2.3	フィッシング対策ガイドライン等の改定作業	44
6.2	フィッシング対策協議会の会員組織向け活動	44
6.2.1	運営委員会開催	44
6.2.2	ワーキンググループ会合等 開催支援	44
第 7 章	広報活動	45
7.1	講演	45
7.2	協力・後援	46
7.3	公開資料	46
7.3.1	ソフトウェア等の脆弱性関連情報に関する届出状況	46
7.3.2	公式ブログ「JPCERT/CC Eyes」	46
付録 A	インシデントの分類	48

トピックス&ハイライト

JPCERT/CC 創立 30 周年

JPCERT/CC は、2026 年 10 月に創立 30 周年を迎えました。代表理事の菊池浩明からのメッセージを Web サイトに掲載していますので、ぜひご覧ください^{*1}。この機会に、設立の年に雑誌に載った対談を手がかりとして、この 30 年を振り返ってみます。

JPCERT/CC の始まりは、インターネット技術者の有志による活動でした。1990 年代の初め、米国の CERT/CC から届くセキュリティ情報を、関連組織の技術者がボランティアで国内に流していました。やがて商用インターネットサービスが始まり、利用者が一気に広がると、有志の手には負えなくなりました。インシデントに対応するための組織が必要だと考えた仲間が集まり、通商産業省（当時）の動きとも重なって、1996 年 10 月、JPCERT/CC は活動を始めました。そのいきさつは、10 周年の折に書き記しました^{*2}。

変わるもの

設立から 1997 年 9 月末までの約 1 年間に JPCERT/CC が受け付けた被害報告は 383 件でした^{*3}。今では、一つの四半期だけで 1 万件を超える報告が寄せられます。インターネットは一部の人のものから社会の基盤になり、攻撃する側も、腕試しのいたずらから、金銭目当ての犯罪や国家の関与が疑われるものへと変わりました。

組織も大きくなりました。2003 年には法人格を取得し、石田晴久先生の後を受け、山口英が初代の代表理事に就きました^{*4}。設立から間もないころに 8 人だった常勤スタッフは^{*5}、今では 100 人近くに増えました。これまでに在籍した職員は 400 人近くに上ります。ここを巣立ち、国内外のセキュリティの現場で活躍している人も少なくありません。

JPCERT/CC を取り巻く社会も、大きく変わりました。設立のころ、セキュリティを専門に扱う会社

^{*1} 菊池浩明. “JPCERT/CC 30 周年を迎えて”. JPCERT/CC. <https://www.jpcert.or.jp/30th-anniversary.html>, (2026-10-01)

^{*2} 歌代和正. “JPCERT/CC 立ち上げのころの話”. JPCERT/CC. <https://www.jpcert.or.jp/magazine/10th/beginning.html>, (2009-06-19)

^{*3} “インターネットのセキュリティ問題と JPCERT/CC”. JPCERT/CC, IP Meeting 1997. <https://www.nic.ad.jp/ja/materials/iw/1997/proceedings/IPM-PDF/jpcert.pdf>

^{*4} “コンピュータ緊急対応センターが中間法人化”. JPCERT/CC. <https://www.jpcert.or.jp/press/2003/0501.pdf>, (2003-05-01)

^{*5} 大林正英. “歴史的一幕 10 年前 コンピュータ緊急対応センターの設立”. JPNIC Newsletter No.34, pp.10-11. https://www.nic.ad.jp/ja/newsletter/No34/NL34_0310.pdf, (2006-11)

や組織はごく限られていました。今ではセキュリティを本業とする会社が数多く生まれ、企業や団体にも、インシデントに対応する CSIRT や、製品の脆弱性に対応する PSIRT が置かれるようになりました。2007 年に 6 チームで発足した日本シーサート協議会は*⁶、今では加盟チームが 600 を超えています*⁷。世界のインシデント対応チームが集う FIRST には、JPCERT/CC が 1998 年、日本で初めて加盟しました*⁸。日本からの加盟は今では 50 チームに上り、国別では米国、スペインに次ぐ数です*⁹。業界内でセキュリティ情報を共有する ISAC も設けられました。国も、内閣官房に司令塔を置いて体制を整え*¹⁰*¹¹、行政の情報システムについては、デジタル庁が安全の基準づくりを担うようになりました*¹²。セキュリティは、一部の技術者の関心事から、経営や社会全体の課題へと広がりました。

変わらないもの

それでも、JPCERT/CC が中立的な調整役であることに変わりはありません。一つのインシデントには、被害を受けた組織、踏み台にされた組織、製品の開発者など、立場の違う多くの当事者が関わり、国境を越えることも珍しくありません。誰かの命令で片づくものではなく、当事者の間を取り持つ役割が欠かせないのです。

設立の年、雑誌の企画で、共に立ち上げに関わった佐野 晋と対談しました*¹³。佐野はそこで、インターネットには権力でコントロールする仕組みがない以上、独自の解決の方法が必要だと語っています。政府にも行政にも民間にもセキュリティが浸透した今も、その答えは変わっていないと思います。

この原稿を書いている間にも、国内の組織への攻撃が相次ぎ、連日のように報じられています。しかし、どこから侵入され、どのような手口が使われたのかという技術的な情報は、被害を受けた組織の外にはなかなか出てきません。

対談のあとには、二人がそれぞれ短い文章を寄せています。佐野の文章には、こうあります。

不正アクセスの実態・被害総額などが公表されていない状態では、十分な動機をもてず、不十分な対策しか行なえない組織が多いのが現状です。

この 30 年で、被害そのものは公表されるようになりました。変わらないのは、対策に必要な情報が当事者の手元にとどまる構図です。情報が集まらなければ、調整役は動けません。

同じ対談では、両方の利用者がメールをやり取りできるよう、パソコン通信とインターネットを相互接

*⁶ “沿革”. 日本シーサート協議会. <https://www.nca.gr.jp/outline/history.html>, (2026-10-09 閲覧)

*⁷ “会員一覧”. 日本シーサート協議会. https://www.nca.jp/M10/corporate_list, (2026-10-09 閲覧)

*⁸ “About JPCERT/CC”. JPCERT/CC. <https://www.jpcert.or.jp/english/about/>, (2026-06-24)

*⁹ “FIRST Members around the world”. FIRST. <https://www.first.org/members/map>, (2026-10-09 閲覧)

*¹⁰ “政府全体での情報セキュリティ対策”. 平成 17 年版 情報通信白書. 総務省. <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h17/html/H3702200.html>, (2005)

*¹¹ “国家サイバー統括室発足式”. 首相官邸. <https://www.kantei.go.jp/jp/103/actions/202507/01hossokushiki.html>, (2025-07-01)

*¹² “サイバーセキュリティ”. デジタル庁. <https://www.digital.go.jp/policies/security>, (2026-04-07)

*¹³ 特別対談 “「対策基準」作成と JPCERT/CC 設立 不正アクセスに緊急対策すむ” (出席者：歌代和正、佐野晋). 『安全と管理』1997 年 2 月号, pp.24–27. 本文中の対談からの引用は、すべてこれによります。引用にあたり、一部の表現を改めています。

*¹⁴ この画像は、誌面に掲載された低解像度の写真をもとに生成 AI で再構成したものです。細部は元の写真よりかなり盛られている可能性があります。



図 1 『安全と管理』 1997 年 2 月号の特別対談（右が佐野、左が歌代）^{*14}

続したときのことも話題になりました。パソコン通信の中で閉じていれば、通信内容が途中で漏れる心配はありませんでしたが、インターネットに送り出すと、そうはいかなくなったのです^{*15}。対策を立ててから開放すべきだったのでは、と水を向けると、佐野はこう答えています。

時代はやはり相互接続を優先したのでしょう。（中略）危険は承知の上で、メリットを享受することになりました。

対策を整えてから使い始める、という順番は、現実には守られません。普及してから危険に気付くことも少なくありません。便利さが先に走り、安全が後から追いかけます。JPCERT/CC は、その追いかける側の仕組みとして生まれました。

そして今、同じことがはるかに大きな規模で起きています。生成 AI は、危険が十分に理解されるより先に、それを上回る便利さによって社会の隅々へ入り込もうとしています。インターネットの普及で社会が一変する様子を間近で見ましたが、AI がもたらそうとしている変化は、それ以上のものになるようにも感じられます。

佐野は常々、2 本の線のグラフを描いては、「利便性と安全性はトレードオフで、いい落とし所を見つけないければならない。でも、技術によって全体を高めることができるんだ」と語っていました。その時々何を守り、どのリスクを許容するかを見極めながら、時間をかけてよりよい方向へ進んでいく、ということなのでしょう。

続くもの

当時 ISP にいた私は、自分たちが運用するネットワークの安全に責任を持つのは当然だと考えていました。その一方で、利用者には「最終的に信用できるのは自分だけで、ISP なんか信じてはいけない」とも言っていました。顧客向けにセキュリティサービスを提供していながら、です。

私も、対談のあとに寄せた文章で、コンピューターセキュリティにはこうした矛盾がつきまとう、と書き

^{*15} 当時は、インターネットに接続する組織が第三者の通信を中継することもあり、通信の暗号化も一般的ではありませんでした。現在は暗号化が広く使われ、事情は大きく異なります。

ました。今の言葉で言えば、ゼロトラストにも通じる考え方です。当時は矛盾として書いたことが、30年を経て、当たり前の考え方になりつつあります。クラウドサービスがランサムウェアの被害に遭い、預かっていた顧客のデータが失われる事態も、現実起きています。最後に頼れるのは自分だけ、という言葉は、残念ながら今も通用します。

一方で、JPCERT/CCの仕事は信頼の上に成り立っています。報告を寄せてもらえるのも、連絡した先が動いてくれるのも、互いの信頼があってこそです。簡単に人を信じるなど説きながら、信頼なしには立ち行かない。JPCERT/CCは、その矛盾を抱えたまま30年間活動してきたことになります。

先の文章は、こう結んでいます。

そんなわけで、まだしばらくは矛盾と付き合い続けることになるのでしょう。

「まだしばらく」と書いた時間は、30年になりました。この矛盾は、おそらくこれからも解消しないでしょう。

残念なことに、同志の佐野さんは2020年に鬼籍に入りました^{*16}。設立時に代表をお願いした石田晴久先生^{*17}、JEPG/IPの時代から活動の中心にいた山口英さん^{*18}、2006年から常務理事としてCSIRTの普及と国際連携に力を尽くした早貸淳子さん^{*19}と、多くの人を失いましたが、これからも我々の活動を見守ってくれていると思います。

JPCERT/CCの30年は、報告を寄せてくださる方々、連絡に応じて対処してくださる方々、国内外の仲間たち、そしてここで働き、巣立っていった多くの人たちとの信頼のつながりに支えられてきました。そのつながりは、これからも続いていくと信じています。皆さまに、心より御礼申し上げます。

(歌代和正)

^{*16} “訃報：JPNIC 理事 佐野晋氏”。JPNIC. <https://www.nic.ad.jp/ja/topics/2020/20200116-01.html>, (2020-01-16); 歌代和正. “佐野 晋さんを悼んで”. JPCERT/CC Eyes. <https://blogs.jpcert.or.jp/ja/2020/01/rip.html>, (2020-01-30); 「佐野晋さんお別れの会」企画検討チーム編. “FYI: 佐野さんが教えてくれたたくさんさんのこと”. (2020-09-30)

^{*17} 村井純. “名誉会員 石田晴久博士を偲ぶ”. 『情報処理』Vol.50 No.4, pp.353-354. <https://ipsj.ixsq.nii.ac.jp/records/60553>, (2009-04)

^{*18} “訃報 JPCERT/CC 理事 山口 英氏”. JPCERT/CC. <https://www.jpcert.or.jp/about/2016/PR20160512R.html>, (2016-05-12)

^{*19} “訃報 JPCERT/CC 理事 早貸 淳子氏”. JPCERT/CC. <https://www.jpcert.or.jp/press/2026/PR20260105.html>, (2026-01-05)

第 1 章

インシデント対応支援および脅威情報分析

1.1 インシデント対応支援

JPCERT/CC では、国内外で発生するインシデントの報告を受け付けています*¹。本節では、本四半期に受け付けたインシデント報告について、統計など定量的にまとめた統計データと、特筆すべき事例を紹介します。

1.1.1 四半期の統計情報

本四半期のインシデント報告件数、報告されたインシデントの総数および報告に対応して JPCERT/CC が行った調整の件数を月別に表 1.1*²に示します。

本四半期に寄せられた報告件数は 12,932 件でした。このうち、JPCERT/CC が国内外の関連する組織に対して行った調整件数は 4,048 件でした。報告件数は前四半期の 14,056 件に比べて 8% 減少、調整件数は前四半期の 3,398 件に比べて 19% 増加しました。また、報告件数は前年同期の 23,857 件に比べて 46% 減少、調整件数は前年同期の 3,257 件に比べて 24% 増加しました。

表 1.1 インシデント報告等の月別件数

項目	7 月	8 月	9 月	合計	前四半期合計
報告件数	3,903	4,487	4,542	12,932	14,056
インシデント件数	3,183	2,864	2,708	8,755	9,305
調整件数	1,311	1,403	1,334	4,048	3,398

*¹ JPCERT/CC では、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピューターのセキュリティに関わる事件、できごとの全般をインシデントと呼んでいます。

*² 報告件数は、報告者から寄せられた Web フォーム、メールによる報告の総数を示します。インシデント件数は、各報告に含まれるインシデント件数の合計を示します。一つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。調整件数は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

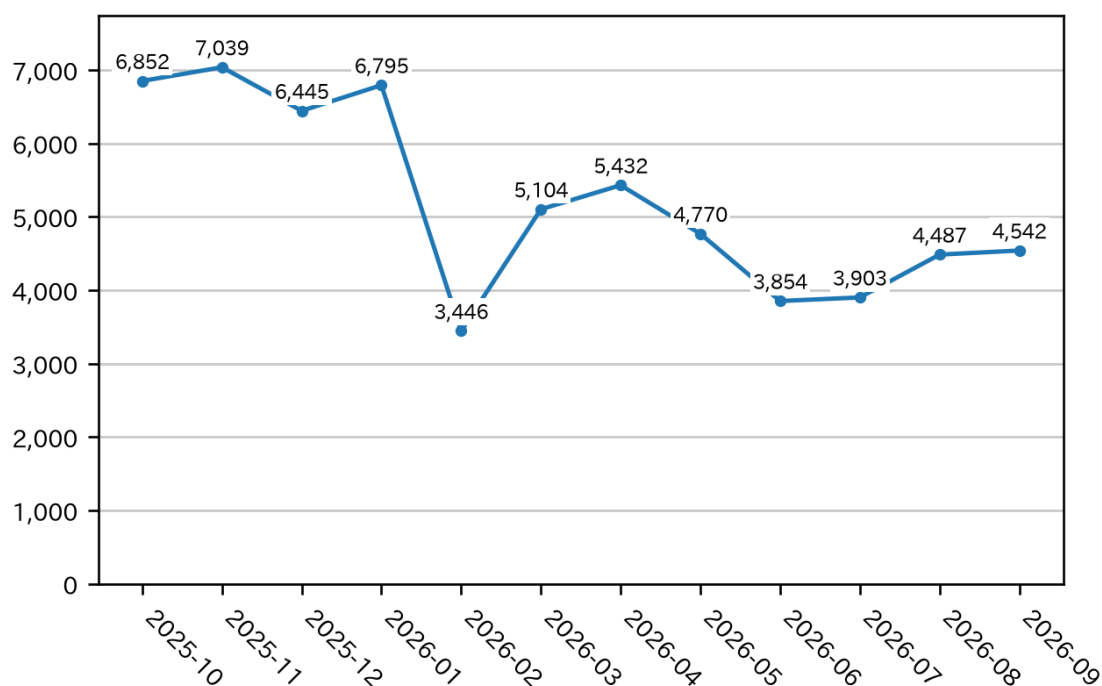


図 1.1 インシデント報告件数の推移

表 1.2 インシデント件数のカテゴリー別内訳

インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	2,759	2,404	2,020	7,183	8,313
Web サイト改ざん	116	194	293	603	181
マルウェアサイト	5	7	19	31	21
スキャン	98	81	85	264	190
DoS/DDoS	0	0	0	0	1
ランサムウェア	2	2	2	6	8
制御システム関連	1	0	0	1	1
標的型攻撃	1	1	2	4	8
その他	201	175	287	663	582

図 1.1 と図 1.2 に報告件数および調整件数の過去 1 年間の月次の推移を示します。

JPCERT/CC では、報告を受けたインシデントをカテゴリー別に分類し、カテゴリーに応じた調整、対応を実施しています。各インシデントの定義については付録 A インシデントの分類をご参照ください。本四半期に報告を受けたインシデント件数のカテゴリー別内訳を表 1.2、カテゴリー別割合を図 1.3 に示します。

フィッシングサイトに分類されるインシデントが 82.0%、スキャンに分類される、システムの弱点を探索するインシデントが 3.0% を占めています。

図 1.4 から図 1.7 に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンの各イン

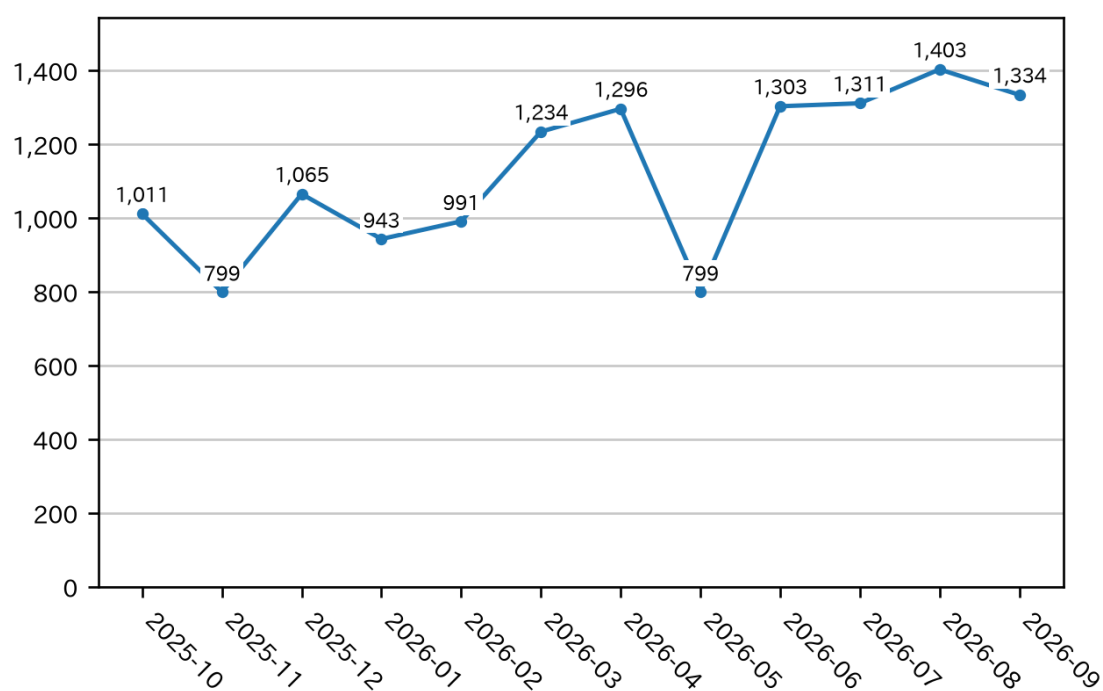


図 1.2 インシデント調整件数の推移

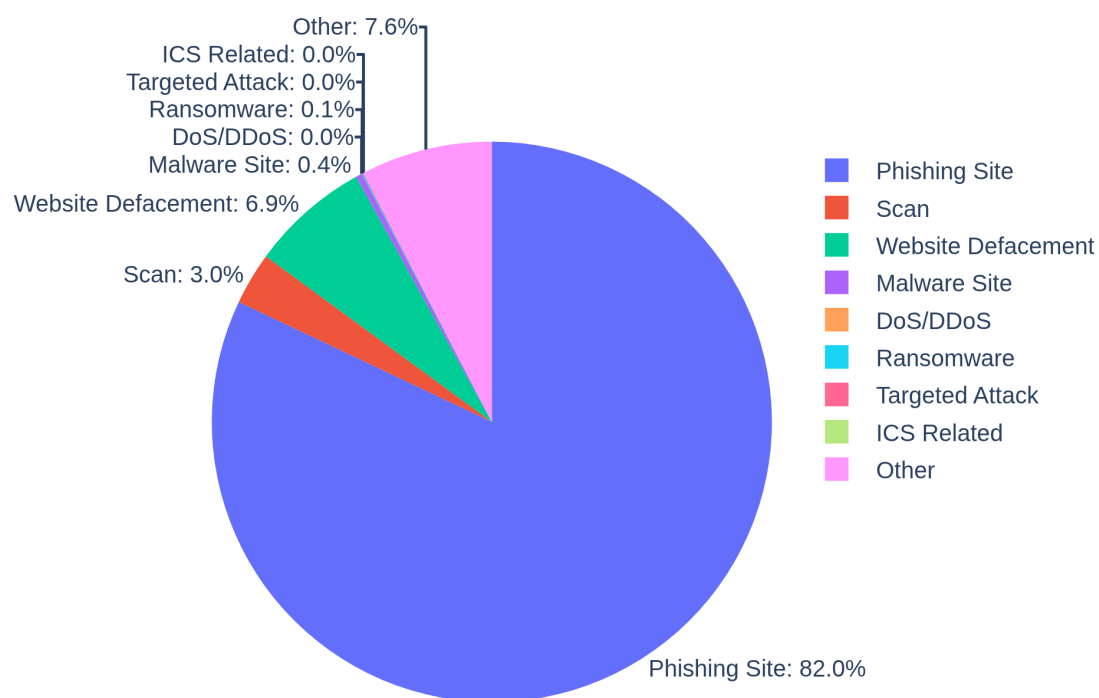


図 1.3 インシデント件数のカテゴリー別割合

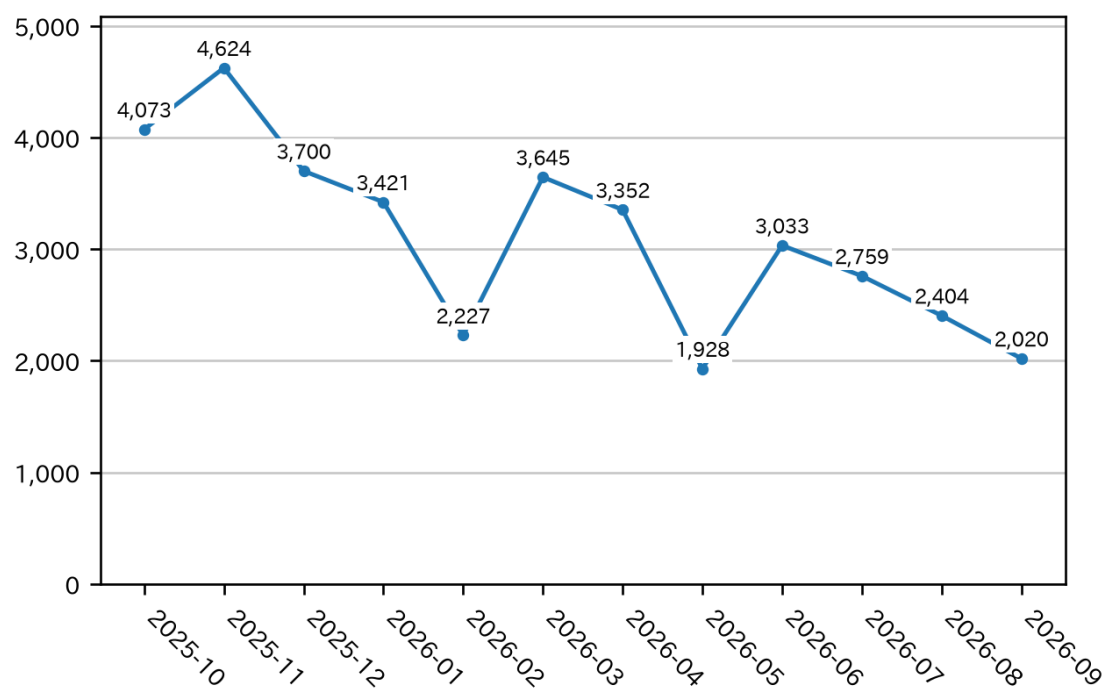


図 1.4 フィッシングサイト件数の推移

シデントの過去 1 年間の月次の推移を示します。

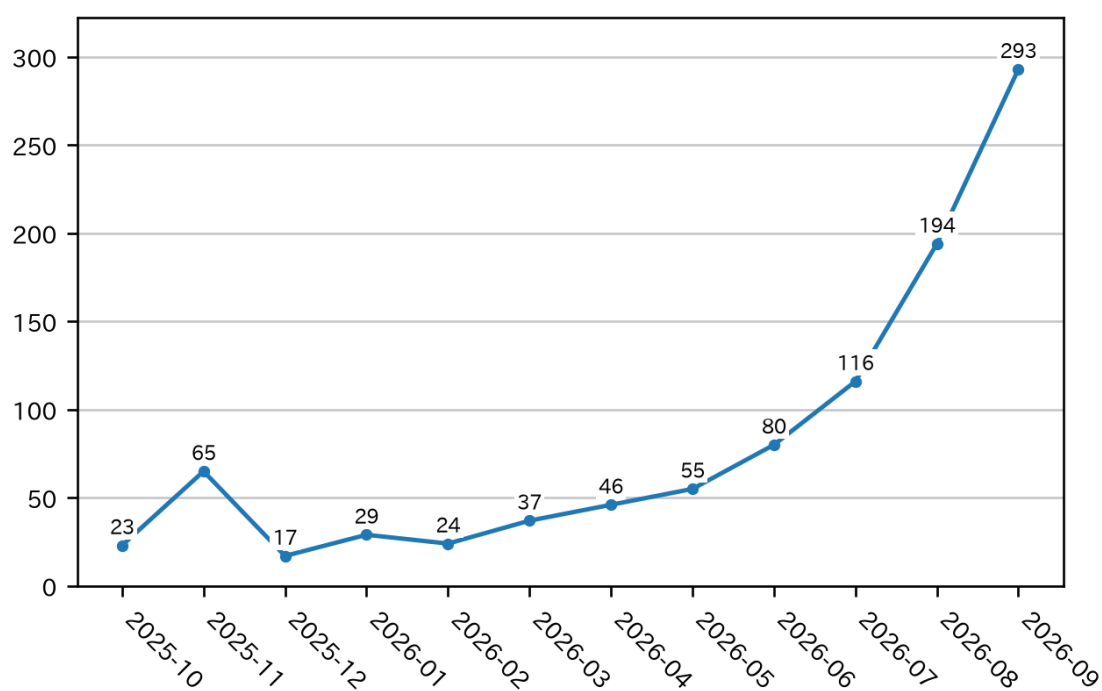


図 1.5 Web サイト改ざん件数の推移

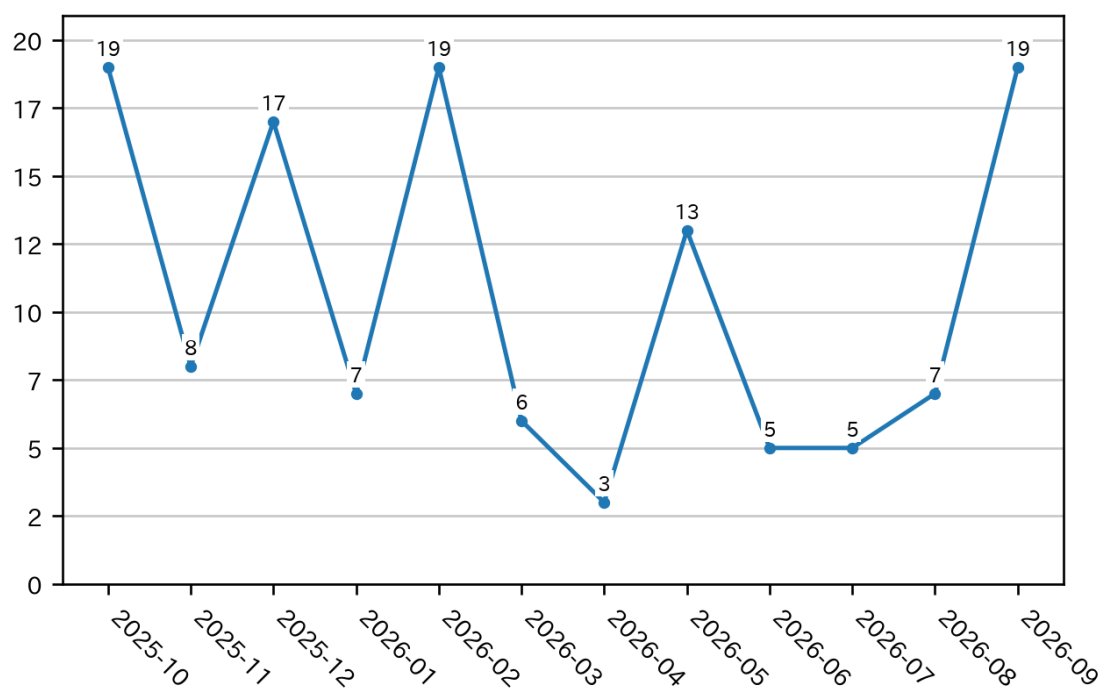


図 1.6 マルウェアサイト件数の推移

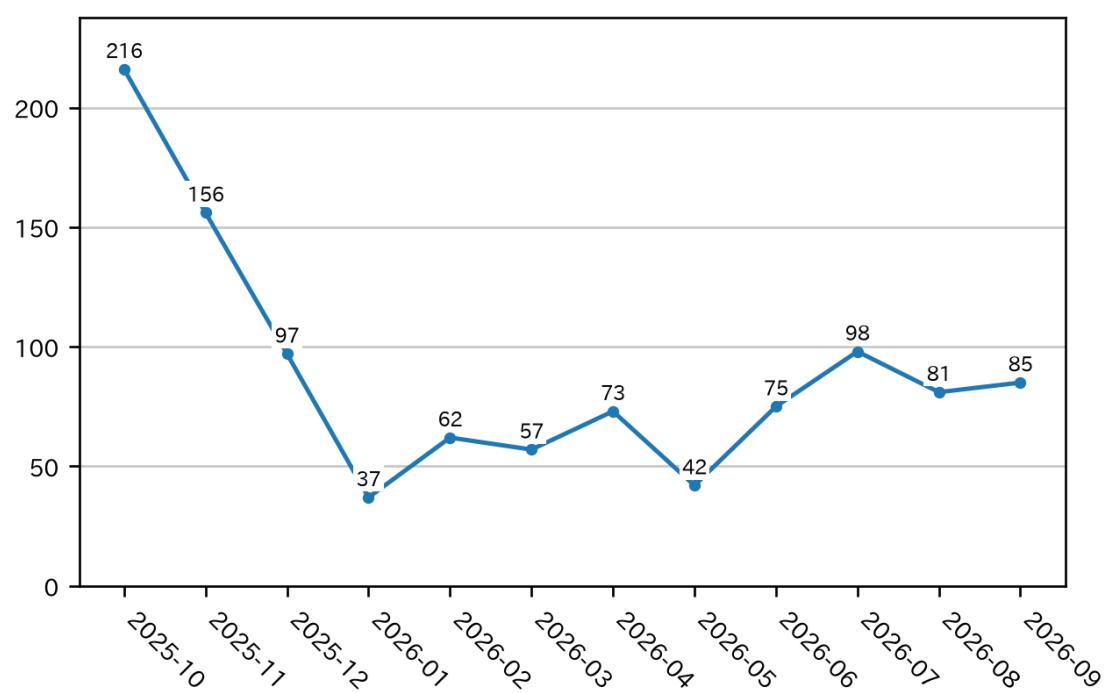


図 1.7 スキャン件数の推移

表 1.3 ブランドの国内外別によるフィッシングサイト件数の内訳

フィッシングサイト	7月	8月	9月	合計	割合
国内ブランド	1,682	1,532	1,418	4,632	64%
国外ブランド	308	528	297	1,133	16%
ブランド不明	769	344	305	1,418	20%
全ブランド合計	2,759	2,404	2,020	7,183	

1.1.2 インシデントの傾向

1.1.2.1 フィッシングサイトの傾向

本四半期に報告が寄せられたフィッシングサイトの件数は 7,183 件で、前四半期の 8,313 件に比べて 14% 減少しました。また、前年同期の 9,063 件に比べて 21% 減少しました。

本四半期は、国外のブランドを装ったフィッシングサイトの件数は 1,133 件で、前四半期の 1,088 件に比べて 4% 増加しました。また、国内のブランドを装ったフィッシングサイトの件数は 4,632 件で、前四半期の 5,974 件に比べて 22% 減少しました。

本四半期のブランドの国内外別によるフィッシングサイト件数の内訳を表 1.3^{*3}に、国外ブランドと国内ブランドそれぞれのフィッシングサイト件数の業界別の割合を図 1.8 と図 1.9 に示します。

JPCERT/CC が報告を受けたフィッシングサイトのうち、国外ブランド関連の報告では E コマースサイトを装ったものが 80.2%、国内ブランド関連の報告では金融関連のサイトを装ったものが 65.7% で、それぞれ最も多くを占めました。

国外ブランドでは、Amazon や Apple Account を装ったフィッシングサイトが多くを占めました。国内ブランドでは、Vpass や三井住友カードを装ったフィッシングサイトが増加した一方で マネックス証券や SBI 証券、JCB を装ったフィッシングサイトは大きく減少しました。

特に、2026 年 8 月から 2026 年 9 月にかけて、Vpass が実施したキャンペーンサイトを模倣したフィッシングサイトが急増しました。このフィッシングサイトでは、キャンペーンに当選した旨を表示して利用者を誘導し、商品の送付先の確認などとしてクレジットカード情報の入力を求める手口でした。

^{*3} **ブランド不明**は、報告されたフィッシングサイトが確認時に停止していた等の理由により、ブランドを確認することができなかったサイトの件数を示します。

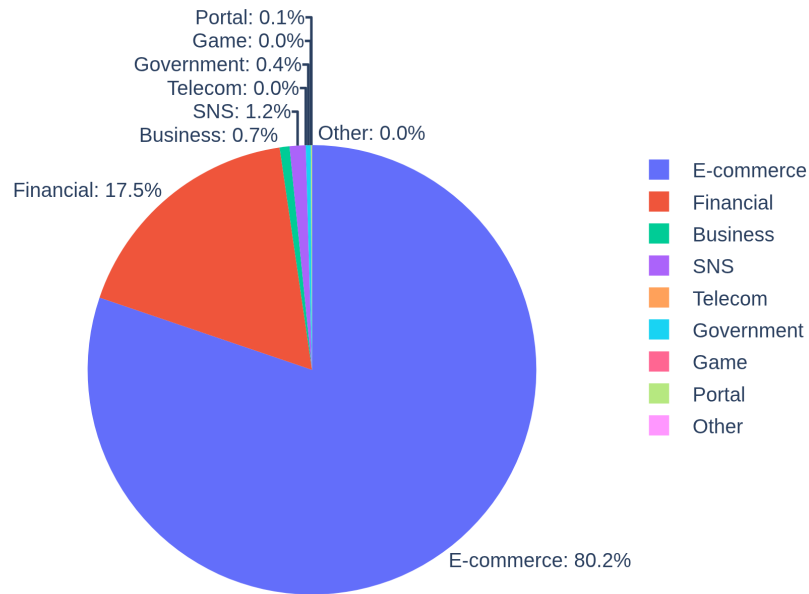


図 1.8 国外ブランドのフィッシングサイトの件数の業界別の割合

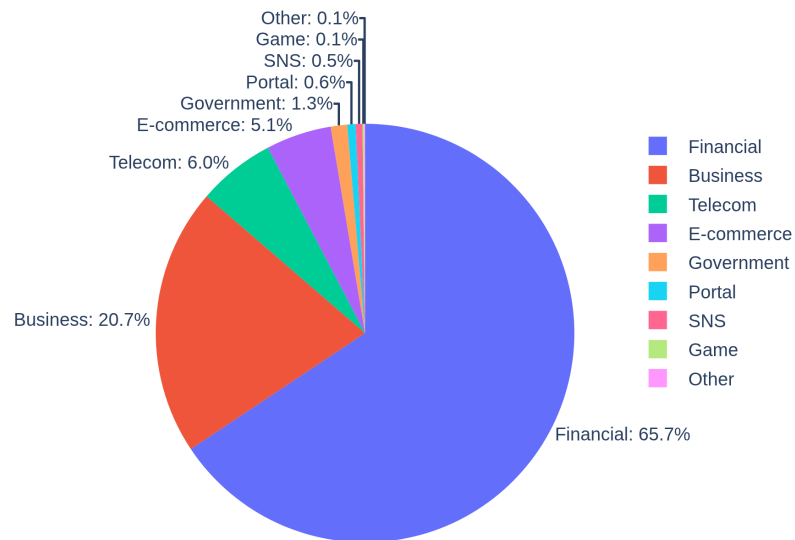


図 1.9 国内ブランドのフィッシングサイトの件数の業界別の割合

1.1.2.2 Web サイト改ざんの傾向

本四半期に報告が寄せられた Web サイト改ざんの件数は 603 件でした。前四半期の 181 件に比べて 233% と大幅に増加しました。

正規 Web サイトに海外オンラインカジノサイトなどのリンクが大量に埋め込まれた事例

国内の複数の正規 Web サイトが改ざんされ、海外のオンラインカジノサイトなどへのリンクを含む HTML が非表示の状態でも 5,000 行以上埋め込まれていました。これは、正規 Web サイトに攻撃者が売り込みたい Web ページへのリンクを埋め込むことによって、後者が前者から参照されているように見せかけて、検索エンジンによる後者の Web ページとしての評価を高めようとする不正な SEO 行為と考え

られます。

外部から取得したコードを実行する JavaScript が EC サイトに埋め込まれた事例

EC-CUBE で構築された国内の複数の EC サイトが改ざんされ、C2 サーバーから取得したコードを実行する JavaScript が埋め込まれていました。C2 サーバーとの通信には、WebRTC または WebSocket が使用されていました。また、当該 EC サイトへアクセスしたユーザーのアクセス先 URL が購入画面であることを判定する処理も確認されており、クレジットカード情報などの窃取を目的としていた可能性があります。

1.1.2.3 標的型攻撃の傾向

標的型攻撃に分類されるインシデントの件数は 4 件でした。

マルウェア LotusLite への感染を狙った標的型攻撃メール

本四半期は、LotusLite と呼ばれるマルウェアに感染させようとする標的型攻撃メールを確認しました。標的型攻撃メールに記載された Google ドライブのリンクにアクセスすると、VHDX ファイルをダウンロードさせられます。VHDX ファイル内には PDF ファイルに偽装した実行ファイルが含まれており、このファイルを実行すると SolidPDFCreator.exe という正規ファイルが SolidPDFCreator.dll という不正な DLL をロードし、マルウェアに感染します。

1.1.2.4 その他のインシデントの傾向

本四半期に報告が寄せられたマルウェアサイトの数は 31 件でした。前四半期の 21 件に比べて 48% 増加しています。

本四半期に報告が寄せられたスキャン件数は 264 件でした。前四半期の 190 件に比べて 39% 増加しています。

スキャンの対象となったポートのトップ 10 を表 1.4 に示します。頻繁にスキャンの対象となったポートは、Telnet (23/TCP)、SSH (22/TCP)、HTTP (80/TCP)、SMTP (25/TCP) でした。

その他に分類されるインシデントの件数は 663 件でした。前四半期の 582 件に比べて 14% 増加しました。

1.2 脅威情報の分析と提供

JPCERT/CC は、インシデントなどによる被害の発生や拡大を防ぐために、脆弱性情報や脅威情報、セキュリティ情報などを収集・分析しています。分析の結果、インシデントなどによる被害の発生や拡大に対する蓋然性が高まったと判断した場合、「注意喚起」や「早期警戒情報」などの警戒情報やインシデントへの対処・対策のための情報を提供しています。

表 1.4 ポート別のスキャン件数のトップ 10

ポート	7 月	8 月	9 月	合計
23/tcp	16	21	19	56
22/tcp	12	13	17	42
80/tcp	12	11	11	34
25/tcp	0	8	2	10
52869/tcp	10	0	0	10
143/tcp	8	0	0	8
8081/tcp	4	0	4	8
8443/tcp	0	5	2	7
82/tcp	0	2	4	6
2194/tcp	3	0	3	6

1.2.1 情報収集・分析

JPCERT/CC が収集・分析する情報には、自ら収集した情報に加え、ご報告いただいた国内外で発生するインシデントの情報や、各地域や組織の CSIRT などから共有された情報も含まれます。それらをもとに、インシデントの発生や拡大の可能性を分析しています。

また、JPCERT/CC が提供した情報に対する各組織からのフィードバックなどを収集し、国内での影響把握とさらなる情報の分析に役立てています。特に、情報共有プラットフォーム「CISTA（Collective Intelligence Station for Trusted Advocates）」（1.2.3 参照）を介した各組織からのフィードバックは、他組織へも展開するなど有効活用しています。

1.2.2 Web サイトでの情報提供

JPCERT/CC は、Web サイトで「注意喚起」や「CyberNewsFlash」「Weekly Report」などの情報を公開しています。RSS フィードを提供するとともに、JPCERT/CC が運用する情報配信用メーリングリストの登録者（本四半期末時点で約 43,000 名）には、一部の情報をメールでも配信しています。

1.2.2.1 注意喚起

深刻かつ影響範囲の広い脆弱性などが公表された場合には、「注意喚起」を公開し、利用者に対して広く対策を呼びかけています。

- JPCERT/CC 注意喚起
<https://www.jpcert.or.jp/at/>

本四半期は、12 件公開または更新しました。

- 2026-07-15

2026 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起

- 2026-07-30
Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性（CVE-2026-66066）に関する注意喚起
- 2026-07-31
2026 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起（更新）
- 2026-08-03
Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性（CVE-2026-66066）に関する注意喚起（更新）
- 2026-08-12
2026 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起
- 2026-08-14
Metabase の SQL インジェクションの脆弱性（CVE-2026-72898）に関する注意喚起
- 2026-08-15
NetScaler ADC および NetScaler Gateway におけるリモートコード実行につながる脆弱性（CVE-2026-8452）に関する注意喚起
- 2026-09-09
2026 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起
- 2026-09-09
Adobe Acrobat および Reader の脆弱性（APSB26-141）に関する注意喚起
- 2026-09-15
Cisco Secure Email Gateway における SQL インジェクションの脆弱性（CVE-2026-76461）に関する注意喚起
- 2026-09-24
F5 BIG-IP Access Policy Manager におけるヒープベースのバッファオーバーフローの脆弱性（CVE-2026-94127）に関する注意喚起
- 2026-09-28
NetScaler ADC および NetScaler Gateway における複数の脆弱性（CVE-2026-88771、CVE-2026-88772 等）に関する注意喚起

1.2.2.2 CyberNewsFlash

JPCERT/CC は、公開時点で注意喚起の基準に満たない脆弱性やマルウェア、サイバー攻撃に関する情報などを「CyberNewsFlash」として公開することがあります。

- JPCERT/CC CyberNewsFlash
<https://www.jpcert.or.jp/newsflash/>

本四半期は、1 件公開しました。

- 2026-08-13
JetBrains TeamCity（オンプレミス版）におけるリモートコード実行につながる脆弱性（CVE-2026-63077）について

1.2.2.3 Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の概要をまとめ、原則として毎週水曜日（各週の第 3 営業日）に「Weekly Report」として公開しています。

本四半期は 13 件公開しました。

- JPCERT/CC Weekly Report
<https://www.jpcert.or.jp/wr/>

1.2.3 CISTA での情報提供

JPCERT/CC は、サイバーセキュリティに関する脅威情報や分析・対策情報を、各組織のサイバーセキュリティ関連部門や組織内 CSIRT などの方々が共有する場として、情報共有プラットフォーム「CISTA」を運営しています。CISTA は JPCERT/CC の取り組みにご賛同いただける組織を対象とした登録制です。

CISTA については、次の Web ページをご参照ください。

- CISTA（シスタ）
<https://www.jpcert.or.jp/cista/>

CISTA では、JPCERT/CC が提供した情報に対して、受信した組織がフィードバックや返信を行うことができます。いただいたフィードバックや返信は、許可された共有範囲などに応じて、他組織への情報提供などに活用、還元しています。

1.2.3.1 早期警戒情報

収集した脆弱性情報や脅威情報などのうち、重要な情報インフラなどに重大な影響を及ぼす可能性があり、重要インフラなどを提供する組織に迅速に共有すべきと判断したものを「早期警戒情報」として提供しています。

本四半期は 5 件発信しました。

1.2.3.2 Analyst Note

収集した脆弱性情報や脅威情報などのうち、JPCERT/CC が注目すべきと考えたものを、毎日まとめて「Analyst Note」として提供しています。

本四半期は 61 件発信しました。

1.2.3.3 インディケータ情報

国内の組織に対して行われた攻撃活動のうち、特定の組織や業界を標的としたと考えられるものについては、関係組織の許可を得た上で、把握していない被害の発見や被害防止を目的として、「インディケータ情報」として攻撃を検知するための情報を提供しています。

本四半期は 1 件提供しました。

1.2.3.4 個別提供情報

収集した情報の中から、特定の組織に影響が及ぶと考えられる脆弱性情報および脅威情報について、個別に情報提供を行っています。

例えば、深刻な脆弱性への対策を適用していないなどの「脆弱なホスト」や、すでに脆弱性の悪用によって不正プログラム設置や改ざん、認証情報の窃取がなされている可能性があるホストの利用組織などに対して情報を提供しています。なお、対象の組織へ CISTA で個別に情報を提供できない場合は、JPNIC WHOIS を利用して登録されている連絡先に通知する、あるいは ISP や保守ベンダーに通知を依頼する場合もあります。

本四半期は 71 件提供しました。

1.2.4 対応事例

本四半期に収集した情報、いただいたフィードバックおよび分析した情報、調整・対応した脆弱性や脅威情報のうち、特徴的なものを紹介します。

1.2.4.1 多数の FortiGate の設定から窃取し収集されたとみられる大量の FortiGate 管理者の認証情報

外部から閲覧可能になっている攻撃者管理のサーバーからデータを取得し調査した結果、そのサーバーに Fortinet 製 FortiGate などに関連する多数の認証情報が保存されていたと、海外のセキュリティ研究者が 2026 年 6 月中旬に発表しました。

これを契機に、Hudson Rock や SOCRadar などの海外セキュリティ企業がそれらの認証情報や当該攻撃者に関連する攻撃インフラを調査しました。SOCRadAr は、この攻撃者の活動を「FortiBleed」と命名し、194 カ国の企業や政府機関に属する機器へのログインが可能な 86,644 件を超える認証情報を発見したと報告しました。^{*4} ^{*5} Fortinet は本件について、新たな脆弱性に起因するものではなく、過去のインシデントで漏えいした認証情報や、Fortinet 製品へのブルートフォースなどで収集されたものとの見解を示しました。^{*6} また、窃取した認証情報を、組織の売上高や従業員数、業種などに基づいて分類整理していたことから、SpyCloud は、それらの認証情報を Initial Access Broker (IAB) として商品化しよ

^{*4} “FortiBleed: 75,000 Fortinet Firewalls Compromised: Global Enterprises Exposed - Claim Your Ethical Disclosure”. HudsonRock. <https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure/>, (2026-06-17)

^{*5} “FortiBleed Breach How 80,000+ Corporate Firewalls Were Quietly Compromised”. SOCRadar. <https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/>, (2026-06-16)

^{*6} “Analysis of Reported Credential Compromise of FortiGate Devices”. Fortinet. <https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices>, (2026-06-19)

うとしていたと推定しています。^{*7}

認証情報が悪用された事例として、FortiGate へ侵入した後に、設定情報を取得・解析して認証情報を窃取した事例や、侵害した FortiGate 機器を経由して内部ネットワークの認証トラフィックを傍受し Kerberos や NTLM の認証情報を窃取・解読した事例を、複数の海外セキュリティ企業が報告しています。^{*8} また、INC Ransom および Lynx ランサムウェアが展開された事例を SOCRadar が報告しています。^{*9}

それらの認証情報に国内組織に関連するものが含まれていたため、JPCERT/CC は、国内組織への周知および対応の促進を目的として 2026 年 6 月 23 日に注意喚起を公開しました。^{*10}

その後、SOCRadAr などの複数の海外セキュリティ企業に連絡をし、本件に関するデータを入手・分析しました。その結果、日本に関連する認証情報が 1 万件以上見つかり、その中には Kerberos や NTLM に関係する認証情報も含まれていたことから、国内組織への深刻な被害が発生する恐れがあり、対象組織への通知が必要であると判断しました。

対象組織が多数あったため、影響度を分析して優先順位を定め、個別に通知して対応を促しました。例えば、Kerberos や NTLM に関連する認証情報が漏えいしている組織などを優先して通知しました。

一方、JPCERT/CC だけですべての対象組織に個別に通知することが難しかったことから、国内の関連組織と連携して通知の網羅性向上に努めました。

製品ベンダーの日本法人であるフォーティネットジャパンとも情報共有し、対応方針について協議・調整した上で、連携して対応を進めました。FortiGate 利用組織とベンダーの間にディストリビューターをはじめ、複数の事業者が介在する影響などから、製品ベンダーからの情報が FortiGate 利用組織へ届きにくいなど、緊急情報の伝達に関するサプライチェーンの課題がありました。JPCERT/CC では、こうした課題を踏まえ、被害組織でありながら、製品ベンダーからの通知が届いていないとみられる国内の組織への個別通知を進めました。個別通知先の中には、本件の影響を受けている認識がない FortiGate 利用組織があったほか、FortiGate から設定ファイルが窃取された事例、FortiGate に不審な認証情報が存在していた事例、Kerberos ハッシュや NTLM ハッシュなどの情報も窃取された事例がありました。

本件については、国内組織への侵害が発生しているため、二次被害の防止と根本的な課題の解消に向け、今後も関係組織と調整を図りながら継続して対応を進めていきます。

^{*7} “More Than a Leak: What SpyCloud Found Inside the FortiBleed Threat Actor Infrastructure”. SpyCloud. <https://spycloud.com/blog/what-spycloud-found-inside-the-fortibleed-threat-actor-infrastructure/>, (2026-06-19)

^{*8} “Inside the FortiBleed Open Directory: A Technical Analysis of What the Attacker Left Behind”. CloudSEK. <https://www.cloudsek.com/blog/inside-the-fortibleed-open-directory-a-technical-analysis-of-what-the-attacker-left-behind/>, (2026-06-19)

^{*9} “Is FortiBleed Linked to INC and Lynx Ransomware? All You Need to Know”. SoCRadar. <https://socradar.io/blog/fortibleed-inc-lynx-ransomware-link/>, (2026-07-01)

^{*10} “Fortinet 製品に関連する認証情報の漏えいに関する注意喚起”. JPCERT/CC. <https://www.jpcert.or.jp/at/2026/at260019.html>, (2026-06-23)

1.2.4.2 Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性（CVE-2026-66066）

Ruby on Rails が 2026 年 7 月 29 日、Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性（CVE-2026-66066、通称「KindaRails2Shell」）に関するアドバイザリ^{*11}を公表しました。本脆弱性は Active Storage の画像処理エンジンとして採用されている libvips から継承されたもので、遠隔の第三者によって細工したファイルをアップロードされ、その結果 Ruby on Rails アプリケーションが稼働するサーバー上の `secret_key_base`（Rails が署名・暗号化に使う鍵を生成する際に利用される情報）、データベースやクラウドストレージサービスの認証情報を読み取られる可能性があります。さらに、細工したリクエストに対し、窃取した `secret_key_base` を用いて署名を偽造した上で送信することで、最終的には当該サーバー上でリモートコードの実行に至る可能性があります。

本脆弱性の報告者が公表した技術分析では、悪用の起点となるファイルアップロードは、Active Storage の `direct upload` 機能経由で行われると指摘されていました。`direct upload` 機能はデフォルトで有効となっており、アプリケーション固有の認証・認可を標準では実装していないため、標準の `direct upload` エンドポイントが外部から利用可能な場合、管理画面や API などのユーザー向けアップロード機能を持たないアプリケーションでも、本脆弱性の対象となる可能性があります。JPCERT/CC が本脆弱性の国内への影響を把握するため当該製品の稼働状況を調査したところ、Active Storage 特有のパスから、国内で約 200 台稼働していると推定されましたが、このパスを伴わない利用や Ruby on Rails の国内での普及状況を踏まえると外部からの正確な把握は困難でした。また、本脆弱性に関するエクスプロイトコードが Github に公開されたため、JPCERT/CC は、このコードを検証し、攻撃に使えることを確認しました。これらの状況から、本脆弱性を悪用した不特定多数を狙った攻撃が早期に行われる可能性が高いと判断し、2026 年 7 月 30 日に注意喚起を公開しました。^{*12} その後も、脆弱性発見者の一人と情報連携を行い、精査を進めました。複数の実証コード（Proof-of-Concept）の公開を受けて、開発者がフォレンジック調査用のツールおよびガイドを公開したことから、2026 年 8 月 3 日に注意喚起を更新し、侵害検出方法に関する情報を追記しました。注意喚起の公開に際し、JPCERT/CC は影響を受ける組織が本脆弱性を認知し、修正版への更新や認証情報のローテーションなどの対策を進めることを期待していました。注意喚起の公開後、あらためて稼働状況を調査したところ、稼働しているとみられるホスト数は約 170 件に減少していました。修正版への更新やネットワークアクセスの遮断など具体的な対処の内容までは特定できていませんが、一定数の組織において期待していた対応が進んだものと捉えています。

1.2.4.3 NetScaler ADC および NetScaler Gateway におけるメモリバッファエラーの脆弱性（CVE-2026-8452）

Cloud Software Group が 2026 年 6 月 30 日、Citrix NetScaler ADC および NetScaler Gateway における複数の脆弱性に関するアドバイザリ^{*13}を公表しました。そのうち、CVE-2026-8452 はメモリバッファエラーの脆弱性で、NetScaler ADC および NetScaler Gateway が SAML SP または IdP の構成の

^{*11} “Possible arbitrary file read and remote code execution in Active Storage variant processing”. GitHub. <https://github.com/rails/rails/security/advisories/GHSA-xr9x-r78c-5hrm>, (2026-07-30)

^{*12} “Ruby on Rails の Active Storage におけるリモートコード実行につながる脆弱性（CVE-2026-66066）に関する注意喚起”. JPCERT/CC. <https://www.jpcert.or.jp/at/2026/at260021.html>, (2026-07-30)

^{*13} “NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-8451, CVE-2026-8452, CVE-2026-8655, CVE-2026-10816, CVE-2026-10817, and CVE-2026-13474”. Cloud Software Group. <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604>, (2026-06-30)

場合に影響を受けます。アドバイザリ公表時点では、本脆弱性が悪用された場合、遠隔の第三者によって予期しない動作や誤動作、サービス運用妨害（DoS）状態を引き起こす可能性があると言われていました。その後、海外セキュリティ企業が 2026 年 8 月 14 日に本脆弱性を悪用してリモートコード実行が可能であることを示す技術詳細を公表し、日本時間の 2026 年 8 月 15 日深夜に PHP の Webshell 設置に至るエクスプロイトコードを公開したため、当該コードを使用した攻撃が広く実施される懸念が高まりました。

JPCERT/CC では、過去に当該製品の脆弱性を悪用する国内への攻撃の発生に関する報告を受けています。そのため、本脆弱性の国内への影響を把握するために当該製品の稼働状況を調べたところ、HTTP レスポンスの特徴から、国内で約 500 台が稼働していることが判明しました。当該調査では、該当するホストが SAML SP または IdP の構成かどうかは外形的に測定不能でしたが、上記の実証コードを使用したさまざまな攻撃が発生した場合、国内組織の内部ネットワークへの侵害につながる恐れがあります。そのため、JPCERT/CC では、2026 年 8 月 15 日に本脆弱性に関する注意喚起^{*14}を公開し、国内の利用者に侵害調査および対策の実施を呼びかけました。なお、注意喚起公開時には、侵害の有無を判定する方法について情報がなかったため、技術詳細やエクスプロイトコードの内容に基づいて、侵害調査方法を掲載しました。

その後、SAML SP および IdP 構成の NetScaler ADC および NetScaler Gateway を使用する国内のホストを特定し、利用組織へ個別に通知しました。通知した組織からは JPCERT/CC からの通知で脆弱性を認知したとのフィードバックもあり、本脆弱性の影響を受ける組織の対策の促進につながりました。

^{*14} “NetScaler ADC および NetScaler Gateway におけるリモートコード実行につながる脆弱性（CVE-2026-8452）に関する注意喚起”。JPCERT/CC. <https://www.jpcert.or.jp/at/2026/at260024.html>, (2026-08-15)

第 2 章

インターネット上の探索活動や攻撃活動に関する観測と分析

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、これをホスティングサービス等を利用することで国内外に複数分散配置した、インターネット定点観測システム「TSUBAME」を構築し運用しています。本システムにより収集されるパケットは、特定の機器あるいは特定のサービス機能を持つ機器を探索するために発信されていると考えられます。JPCERT/CC では、本システムによる継続的な観測を通じて、脆弱性情報、マルウェアや攻撃ツールの情報などと照らしあわせて分析しています。その分析から、インターネットを介した攻撃活動や、攻撃の準備活動等を把握し、グローバルな攻撃活動等の迅速な把握に努めています。

2.1 インターネット定点観測システム「TSUBAME」を用いた観測

「TSUBAME」では、インターネットからセンサーに到達するパケットのうち、ワームの感染活動や弱点探索のためのスキャンなど、セキュリティ上の脅威となるパケット（TCP、UDP および ICMP 等）を収集しています。なお、センサーはハニーポットとは異なり、到達したパケットに対して応答しません。

TSUBAME については、次の Web ページをご参照ください。

- TSUBAME（インターネット定点観測システム）
<https://www.jpcert.or.jp/tsubame/index.html>

2.1.1 TSUBAME 観測動向

頻繁に探索された国内のサービス（宛先ポート番号）のトップ 5 を表 2.1、パケット数の推移を図 2.1 に示します。本四半期に最も多く観測されたパケットは 23/TCP（Telnet）宛で、他のポート番号宛てパケットを常に上回っていました。2 番目から 4 番目の順位は、22/TCP、80/TCP、443/TCP でした。期間中に順位が変動しましたが、これは一時的なパケットの増加によるものとみられます。5 番目には前四半期の 3389/TCP と入れ替わって 8080/TCP が入りました。

国内を対象とした探索活動の探索元地域を、本四半期において活動が活発だった順に並べたトップ 5 を

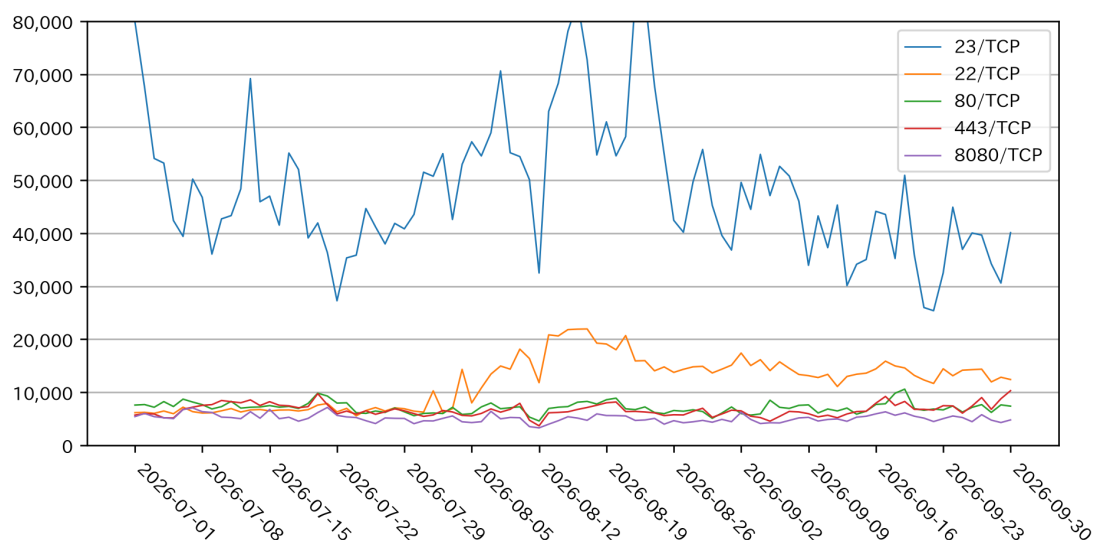


図 2.1 TSUBAME で観測された宛先ポートトップ 5 のパケット数の推移

表 2.1 頻繁に探索された国内のサービス（宛先ポート番号）のトップ 5

順位	宛先ポート番号	前四半期の順位
1	Telnet (23/TCP)	1
2	ssh (22/TCP)	4
3	http (80/TCP)	3
4	https (443/TCP)	2
5	8080/TCP	6

表 2.2 探索元地域トップ 5

順位	探索元地域	前四半期の順位
1	米国 (US)	1
2	オランダ (NL)	2
3	英国 (GB)	3
4	ウクライナ (UA)	TOP10 外
5	ブルガリア (BG)	6

表 2.2 に、パケット数の推移を図 2.2 に示します。

トップは米国、次いでオランダが 2 番目、英国が 3 番目に入りました。4 番目には、2026 年 7 月 5 日から 2026 年 8 月初めにかけてパケット数が増加したウクライナが入りました。ブルガリアは、数日にわたってパケット数が増加する現象が数回見られ、5 番目に入りました。なお、TSUBAME では RIR (Regional Internet Registry) による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

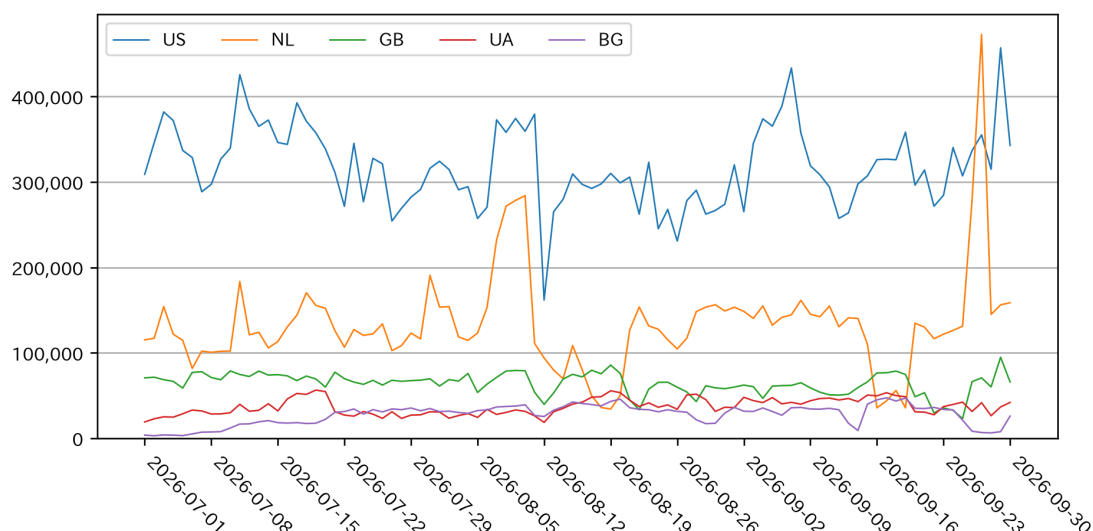


図 2.2 探索元地域からのパケット数の推移

2.1.2 TSUBAME の観測データの活用

前節の TSUBAME 観測動向に書ききれない分析内容や期間中に発生した特徴的な事象については、ブログ「TSUBAME レポート Overflow」で取り上げています。また、JPCERT/CC では、TSUBAME で得た観測データの一部を、組織のシステム管理者の方々がインシデント対応や対策などに活用できるよう、送信元 IP アドレスが割り当てられている関連する組織等に提供しています。

- TSUBAME レポート Overflow
 - TSUBAME レポート Overflow (2026 年 4～6 月)
 - <https://blogs.jpcert.or.jp/ja/2026/07/tsubame-overflow20260406.html>

2.2 ハニーポットの運用とその分析

JPCERT/CC では、HTTP や HTTPS などのサービスに対する通信を記録する低対話型のハニーポットをインターネット上に設置して攻撃者から送られてくる種々の通信内容を収集し、「TSUBAME」の観測結果とあわせて、攻撃活動を分析しています。

2.2.1 AI / LLM 開発者ツールを狙う攻撃活動の観測

前四半期に引き続き、AI / LLM 関連の開発者ツールを標的とした攻撃が継続的に観測されています(図 2.3)。

ペイロードには複数の攻撃手法が見られ、2026 年 8 月下旬を中心に Gradio ライブラリを用いた機械学習アプリケーションへの Python コード注入によるコインマイナー設置、MCP 関連ツール (MCPJam inspector、CVE-2026-23744) や分散処理基盤 (Ray、CVE-2023-48022) の未認証 RCE 悪用など、攻撃の対象が拡大しています。今後も継続することが予想され、注意が必要です。

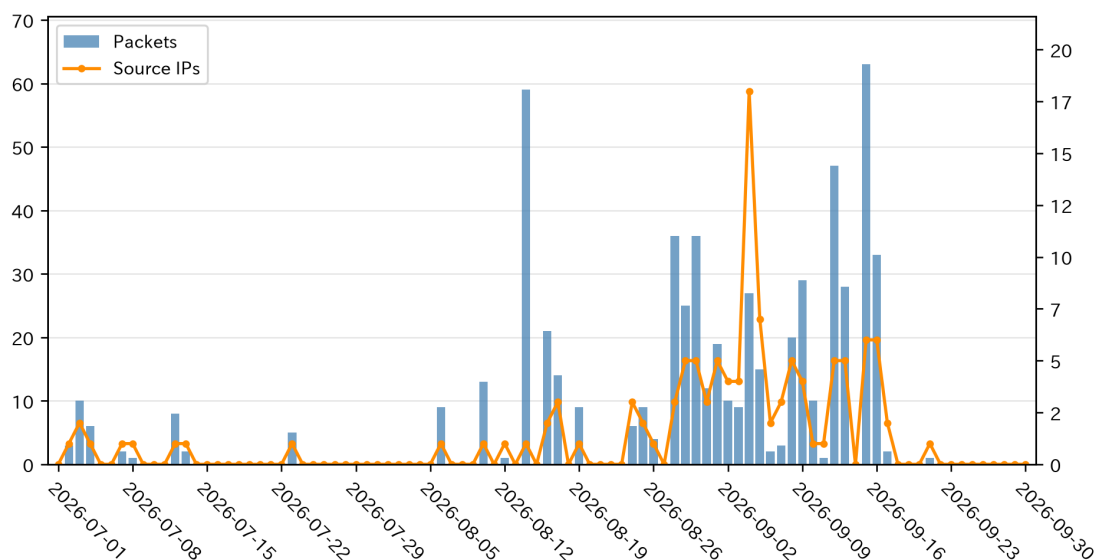


図 2.3 AI / LLM・開発者ツールを狙った攻撃活動の観測数

2.2.2 IoT 機器を標的としたボットネットによるスキャン活動

Mirai 系ボットネットによるとみられるスキャンが、2026 年 7 月 8 日から 2026 年 7 月 12 日にかけて集中的に観測されました。このスキャン活動は主に IoT 機器の既知の脆弱性の悪用を試みるもので、表 2.3 に示す 20 以上の製品が機械的に総当たりされました。

このようなスキャン活動や攻撃活動に対しては、製品のアップデートに加え、サポート終了（EoL）機器の管理インタフェースをインターネットに露出させないようにするなど、多層的な防御を行うことが推奨されます。

表 2.3 標的となった主な IoT 製品と CVE

製品・機器	悪用試行された CVE
TOTOLINK	CVE-2025-60687、CVE-2022-26213、 CVE-2021-43711、CVE-2024-1781 等
Hikvision	CVE-2021-36260
GeoVision	CVE-2024-6047、CVE-2024-11120
Dahua EIMS	CVE-2024-13985
Tenda	CVE-2024-10697、CVE-2022-25438
D-Link	CVE-2015-2051、CVE-2019-8312
PTZOptics	CVE-2024-8956、CVE-2024-8957
Zyxel NWA/NAS	CVE-2024-8234、CVE-2024-6342、CVE-2024-29972
WD My Cloud	CVE-2016-10108
Drobo	CVE-2018-14706
Airspan	CVE-2022-36267
I-O DATA UD-LT1	CVE-2024-52564
MajorDoMo	CVE-2026-27175
Mako Server	CVE-2025-34095
9Router	CVE-2026-59800
WDR201A	CVE-2026-41922、CVE-2026-41925
Advantech EKI	CVE-2024-50374
Ilevia EVE X1	CVE-2025-34513
WePresent	CVE-2025-34103
Synway	CVE-2025-71284
MeiG Smart	CVE-2026-36356

第 3 章

脆弱性関連情報の調整と流通

JPCERT/CC は、ソフトウェア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、脆弱性情報と製品開発者が用意した対策情報を、情報処理推進機構（IPA）と共同運営している脆弱性情報ポータル JVN（Japan Vulnerability Notes）を通じて公表することで広く注意を促す活動を行っています。さらに、脆弱性の作り込みを防ぐためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

3.1 脆弱性関連情報の取り扱い状況

3.1.1 JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC では、寄せられた脆弱性関連情報に対して、関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、製品開発者による脆弱性の検証や対処に向けた調整を行い、JVN を通じて脆弱性情報等を公表しています。また、公表した脆弱性情報の国際的かつ効果的な情報流通のために、CVE（Common Vulnerabilities and Exposures）Program に参加しています。CVE Program は、個々の脆弱性を特定、記述、公表されたものをカタログ化することを使命として、1999 年から専門家コミュニティによって進められてきた国際的な活動です。米国の MITRE が事務局を務めています。JPCERT/CC は、CVE Program において配下の CNA（CVE Numbering Authority、CVE 採番機関）を統括する Root の役割を担うとともに、自ら CNA として CVE 番号を付与しています。

JPCERT/CC は、経済産業省告示「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）に基づく「調整機関」として、製品開発者とのコーディネーションを行っています。調整機関としての活動は、この規程の細目を定めた「情報セキュリティ早期警戒パートナーシップガイドライン（以下「パートナーシップガイドライン」）に沿って、脆弱性情報の「受付機関」である IPA と緊密に連携して進めています。

また、CERT/CC や CISA、NCSC-NL、NCSC-FI といった海外の調整組織との国際調整、国内外から寄せられる報告や調整依頼にも対応しています。

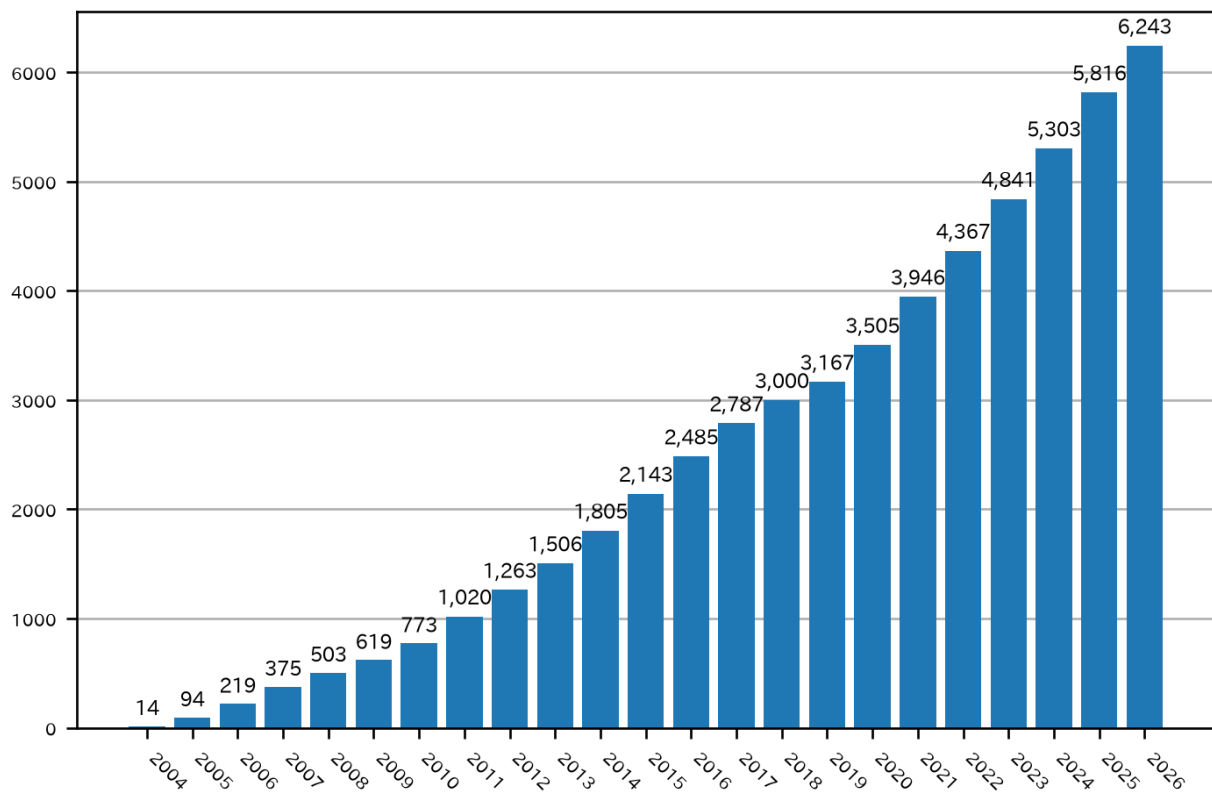


図 3.1 JVN 公表累積件数

3.1.2 Japan Vulnerability Notes (JVN) において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、次の 3 種類に分類されます。

- パートナーシップガイドラインに基づき報告された脆弱性関連情報（「JVN#」に続く 8 桁の数字の形式の識別子を付与している；例：JVN#12345678）
- パートナーシップガイドラインを介さず、報告者、製品開発者、海外の調整機関などから連絡を受けた脆弱性情報（「JNVNU#」に続く 8 桁の数字の形式の識別子を付与している；例：JNVNU#12345678）
- 通信プロトコルやプログラミング言語標準の問題など個別の製品の脆弱性情報という範疇を超えた情報等（「JVNTA#」に続く 8 桁数字の形式の識別子を付与している；例：JVNTA#12345678）

本四半期に JVN において公表した脆弱性情報は 148 件、累積 6,243 件で、累積の推移は図 3.1 のとおりです。

本四半期に公表された個々の脆弱性情報については、次の Web サイトをご参照ください。

- JVN (Japan Vulnerability Notes)
<https://jvn.jp/>

本四半期において公表に至った脆弱性情報の内訳は次のとおりです。

- パートナースhipガイドラインに基づき報告された脆弱性情報に関するもの：46 件
- 国際調整や独自調整に基づく脆弱性情報に関するもの：102 件
- 脆弱性情報に関連する技術情報等に関するもの：0 件

なお、パートナーシップガイドラインに基づく脆弱性関連情報に関する四半期ごとの届け出状況については、次の Web ページをご参照ください。

- 情報処理推進機構（IPA）ソフトウェア等の脆弱性関連情報に関する届出状況
<https://www.ipa.go.jp/security/reports/vuln/software/index.html>

3.1.2.1 特筆すべきパートナーシップガイドラインに基づき報告された脆弱性

本四半期に公表に至った脆弱性のうち、パートナーシップガイドラインに基づき報告された脆弱性の中で、特筆すべきものを紹介します。

JVN#40688603 miChecker における XML 外部実体参照（XXE）に関する脆弱性

- miChecker における XML 外部実体参照（XXE）に関する脆弱性
<https://jvn.jp/jp/JVN40688603/>

本件は、総務省が開発・提供する Web ページのアクセシビリティ評価ツール「miChecker」の脆弱性です。この製品はアクセシビリティ検証作業を支援するもので、その中に動画コンテンツの字幕が適切に提供されているか確認する機能があります。この脆弱性は、細工された字幕ファイルを読み込むと本製品から意図しない通信が発生し、本製品をインストールしている端末内のローカルリソースや内部ネットワークリソースにアクセスされる可能性があるというものです。製品提供元である総務省と調整を開始したところ、現在は総務省からソースコードの寄贈を受けた Eclipse Foundation が製品サポートを担っていることが分かりました。そこで、Eclipse Foundation とも連携して調整を進め、最終的に JVN、総務省、Eclipse Foundation の 3 者がそれぞれアドバイザリを作成し公表しました。製品の「提供」と「開発・サポート」の主体が異なる事例は珍しくありません。JPCERT/CC では、このような場合においても適切な情報公開が行われるよう、各関係者との調整を実施しています。

3.1.2.2 特筆すべき国際調整または独自調整で取り扱った脆弱性

本四半期に公表に至った脆弱性のうち、国際調整または独自調整で取り扱った脆弱性の中で、特筆すべきものを紹介します。

JVNVU#95422936 古野電気製 FA-50（簡易型船舶自動識別装置、AIS）におけるハードコードされた認証情報使用および認証欠如の脆弱性

- 古野電気製 FA-50（簡易型船舶自動識別装置、AIS）におけるハードコードされた認証情報使用および認証欠如の脆弱性
<https://jvn.jp/vu/JVNVU95422936/>

本件は、古野電気が提供する簡易型船舶自動識別装置（AIS）の脆弱性です。この製品は船舶に搭載し、船名や位置などを他の船舶と送受信するための装置で、これまでの脆弱性調整において JPCERT/CC が取り扱った経験のない種類の製品でした。そのため、製品提供者の協力を得て、製品の理解に努めるとともに、脆弱性か否かの判断や、アドバイザリの記述内容に注意を払いました。また、本件の調整においては、報告者と開発者間で脆弱性判断に見解の相違があったため、JPCERT/CC は調整機関として相互理解を促し、両者の合意形成に努めました。加えて本件では、開発者、JVN、CISA の 3 者がそれぞれアドバイザリを公表したため、それぞれの内容や公表日程など、より広範な調整も行いました。今回のように、JPCERT/CC が初めて対応する種類の製品の脆弱性関連情報の調整では、調整機関として視野を広く保ち、製品特性に基づく関係者の見解の違いを受け入れた上で、合意に達するよう調整することが重要であるとの認識を新たにしました。

3.1.3 連絡不能開発者対応

パートナーシップガイドラインに基づいて報告された脆弱性について、製品開発者と連絡が取れないことがあります。このような場合は、パートナーシップガイドラインに規定された連絡不能開発者案件を公表するための手順に沿って対応します。この手順では、公表判定委員会での諮問等を経て公表の可否を判断します。JPCERT/CC はこの手順に基づき、JVN 上で「連絡不能開発者一覧」「Japan Vulnerability Notes JP（連絡不能）一覧」を公表しています。本四半期においては、いずれも新規公表は 0 件です。

- 連絡不能開発者一覧：該当する製品開発者名の連絡先情報を広く求めるための一覧
<https://jvn.jp/reply/>
- Japan Vulnerability Notes JP（連絡不能）一覧：公表判定委員会で公表が妥当と判定された脆弱性を製品利用者に周知するための一覧
<https://jvn.jp/adj/>

3.1.4 CNA および Root としての活動

JPCERT/CC では、CVE Program の活動に参加し、CNA として CVE ID の採番や、Root として国内の製品開発者をスコープとする活動をしています。

2008 年 5 月以降、JVN で公表する脆弱性情報には他の CNA が採番したケースを除き、JPCERT/CC が採番した CVE ID を付与しています。本四半期は、129 件の脆弱性に CVE ID を付与しました。

CNA および CVE については、次の Web ページをご参照ください。

- CNA (CVE Numbering Authority)
<https://www.jpcert.or.jp/vh/cna.html>
- Overview About the CVE Program
<https://www.cve.org/About/Overview>

3.2 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、脆弱性情報流通体制を整備しています。

詳細については、次の Web ページをご参照ください。

- 国内における脆弱性関連情報を取り扱う全ての皆様へ – 情報セキュリティ早期警戒パートナーシップガイドラインに則した対応に関するお願い –
https://www.meti.go.jp/policy/netsecurity/vul_request.html
- 脆弱性情報ハンドリングとは？
<https://www.jpcert.or.jp/vh/>
- 情報セキュリティ早期警戒パートナーシップガイドライン（2026 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2026.pdf
- JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
<https://www.jpcert.or.jp/vh/vul-guideline2019.pdf>

3.2.1 日本国内製品開発者との連携

JPCERT/CC は調整機関として脆弱性情報の提供先となる製品開発者のリストを整備しています。製品開発者に登録をお願いしており、本四半期末時点での登録数は図 3.2 に示すとおり 1,391 です。

詳細については、次の Web ページをご参照ください。

- 製品開発者登録
<https://www.jpcert.or.jp/vh/register.html>

3.2.2 製品開発者との定期ミーティング等の実施

本四半期は 2026 年 8 月 7 日、登録されているすべての製品開発者を対象とした定期ミーティングを開催しました。会場とオンライン配信のハイブリッド形式で、あわせて約 60 名の方にご参加いただきました。本ミーティングでは、製品開発者向けワークショップ企画を含む今後の活動計画案、ソフトウェアサプライチェーンに対する攻撃活動事例、CRA における脆弱性報告と脆弱性コーディネーションとの関係、PSIRT 演習シナリオ作成における生成 AI 活用といったトピックについて説明し、参加者との意見交換を行いました。

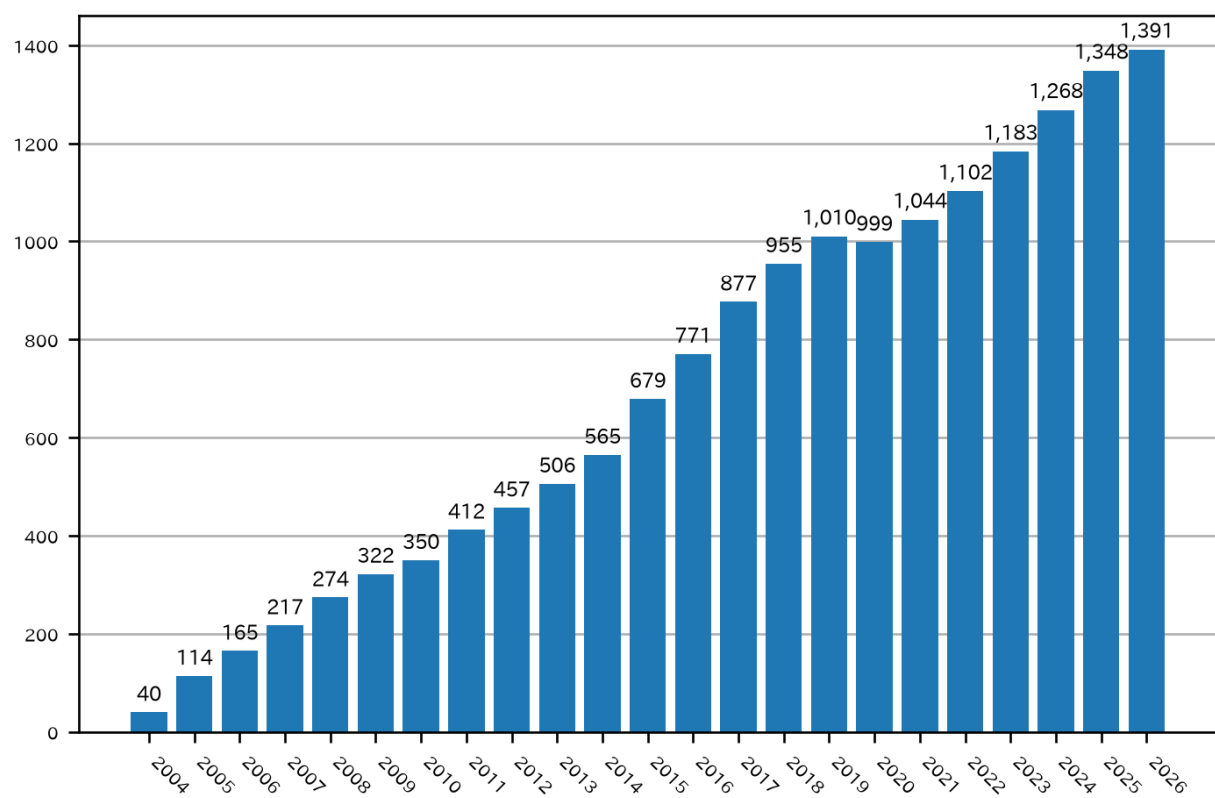


図 3.2 製品開発者登録数

第 4 章

国内連携活動

前章までに述べたような調整業務を円滑に進めるために、各組織の CSIRT やサイバーセキュリティの課題に取り組んでいる業界団体等の協力を必要とする場合があります。そのような場合に備えて、JPCERT/CC では、平時からこれらの組織とセキュリティ状況に関する情報や認識の共有に努め、緊急時の連携が円滑にできるようにするための環境づくりに取り組んでいます。

4.1 業界団体やコミュニティ等との連携活動

サイバーセキュリティに関する取り組みを行っている各業界の ISAC や CEPTOAR などの組織や、業界団体、学会等が開催する集まりに参加し、意見交換や講演等を行っています。本四半期には次のような活動を実施しました。

4.1.1 日本貿易会 ISAC

2026 年 7 月 17 日に開催された技術部会および 2026 年 8 月 21 日に開催された実務部会に参加しました。技術部会では「組織から見たソフトウェアサプライチェーン攻撃」、実務部会では「JPCERT/CC が確認した 2026 年の標的型攻撃事案」というタイトルで講演を行いました。

4.1.2 SICE/JEITA/JEMIMA セキュリティ調査研究合同ワーキンググループ

SICE（計測自動制御学会）と JEITA（電子情報技術産業協会）、JEMIMA（日本電気計測器工業会）が定期的に開催しているセキュリティ調査研究合同ワーキンググループに参加し、制御システムセキュリティに関して専門家の方々と意見を交換しました。

4.1.3 セプターカウンシル運営委員会

JPCERT/CC は、セプターカウンシルの活動に参加しワーキンググループ活動の支援や情報提供等を行うとともに、国家サイバー統括室（NCO）と共同でセプターカウンシルの事務局を支援しています。本四半期は、2026 年 9 月 3 日に開催された第 85 回セプターカウンシル運営委員会で、「FortiBleed」攻撃

事案の状況と対応について情報を共有しました。

4.2 国内関係機関との連携強化および情報交換の環境整備

4.2.1 CISTA 利用組織との連携促進

CISTA 利用組織に対し、CISTA を介した情報共有活動に加えて、情報共有や意見交換のための機会を設けています。対面での会合を開催するなどして組織間の交流を促すとともに、利用組織の方にもご講演いただくなど、対話の活性化に努めています。

なお、本四半期は、新たに 14 組織を CISTA の利用組織として登録しました。

4.2.2 製造業の制御システムセキュリティ担当者向け課題検討グループ

JPCERT/CC では、製造業を中心とした制御システムセキュリティ担当者による課題検討グループを運営しています。このグループでは、制御システムセキュリティに関する共通課題について、JPCERT/CC と登録組織の実務者とが協働し、実践的な検討を行っています。

なお、本四半期末時点で 37 組織が登録されています。

4.3 情報・ツール等の提供

4.3.1 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT (SCADA Self Assessment Tool : 申し込み制) や J-CLICS (制御システムセキュリティ自己評価ツール) を無償で提供しています。

- 日本版 SSAT (SCADA Self Assessment Tool)
<https://www.jpcert.or.jp/ics/ssat.html>
- J-CLICS STEP1 / STEP2 (ICS セキュリティ自己評価ツール)
<https://www.jpcert.or.jp/ics/jclics.html>
- J-CLICS 攻撃経路対策編 (ICS セキュリティ自己評価ツール)
<https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html>

第 5 章

国際連携活動

JPCERT/CC が対応するインシデントの多くが、諸外国の CSIRT や ISP、政府機関との情報共有や協力を必要とします。そのため、JPCERT/CC では、インシデントが発生する前から各国における信頼できるカウンターパートを特定し、いざというときに相互に協力するための信頼関係を築いています。本章では、そのような国際連携活動について、特筆すべき成果を記します。

5.1 海外 CSIRT 構築支援および運用支援活動

JPCERT/CC は、海外の National CSIRT 等のインシデント対応調整能力の向上を図るため、研修会やイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

5.2 国際 CSIRT 間連携

APCERT や FIRST で主導的な役割を担う等、国際的な CSIRT 連携の枠組みにも積極的に参加しています。

5.2.1 APCERT (Asia Pacific Computer Emergency Response Team)

APCERT は 2003 年 2 月に発足したアジア太平洋地域の CSIRT コミュニティーです。JPCERT/CC は、発足時から継続して Steering Committee (運営委員会) のメンバーに選出されており、また、その事務局も担当しています。

APCERT および APCERT における JPCERT/CC の役割については、次の Web ページをご参照ください。

- JPCERT/CC within APCERT
<https://www.jpcert.or.jp/english/apcert/>

5.2.1.1 APCERT Steering Committee 会議の実施

APCERT の Steering Committee は 2026 年 9 月 14 日に電話会議を行い、APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

5.2.1.2 APCERT サイバー演習 (APCERT Drill) 2026 への参加

APCERT Drill は、アジア太平洋地域で発生し国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携強化、ならびにサイバー攻撃により迅速に対応するための APCERT 加盟組織の能力向上を目的として、毎年実施されています。22 回目となる今回のサイバー演習は「Incident Response: RMM-related Compromise (リモートモニタリング・マネージメントツールの侵害への対応)」というテーマで 2026 年 8 月 26 日に実施されました。参加組織は、フォレンジック分析やインシデント対応の手順を確認しました。本演習には、APCERT 加盟組織のうち 18 の経済地域から 23 チームが参加しました。OIC-CERT および AfricaCERT からは 2 チームがゲスト参加しました。JPCERT/CC は、プレーヤー（演習者）として参加するとともに、APCERT 事務局ならびに演習ワーキンググループ (Drill Working Group) のメンバーとして、シナリオの作成や当日の運営において主導的な役割を果たしました。APCERT Drill 2026 についての詳細は、次の Web ページをご参照ください。

- APCERT CYBER DRILL 2026: “Incident Response: RMM-related Compromise”
https://www.apcert.org/documents/pdf/APCERT_Drill_2026_Press_Release.pdf

5.2.2 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しており、2021 年 6 月からは国際部の内田が理事を務めています。本四半期は、毎月のオンライン理事会に加え、2026 年 9 月にインドのムンバイで開催された対面での理事会にも参加しました。

FIRST については、次の Web ページをご参照ください。

- FIRST
<https://www.first.org/>
- FIRST.Org, Inc., Board of Directors
<https://www.first.org/about/organization/directors>

5.3 海外 CSIRT 等の来訪および訪問

本四半期は該当する活動はありませんでした。

5.4 その他国際会議への参加

5.4.1 APNIC 62 に参加・登壇

2026 年 9 月 4 日から 2026 年 9 月 10 日にかけて、インドのムンバイで APNIC 62 が開催されました。これはアジア太平洋地域のインターネットやネットワーク関連事業者、政府関係者、産業関係者などが集まり、インターネット運用に関するポリシー等について議論する会議です。JPCERT/CC はこの会議で基調講演を行い、インシデント対応や CSIRT 間連携に必要な信頼関係の醸成やコミュニティ活動の重要性について訴えました。また、FIRST と APNIC が共催するサイバーセキュリティに関するセッション FIRST-APNIC Technical Colloquium にも登壇し、JPCERT/CC が参加する FIRST DNS Abuse SIG の活動内容を紹介しました。

- APNIC 62

<https://conference.apnic.net/62/>

5.5 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改訂に、情報処理学会の情報規格調査会を通じて参加しています。

本四半期は、2026 年 9 月に WG3 の国際会議がオンライン形式で開催されました。改訂作業中の ISO/IEC 29147（脆弱性情報公開）ならびに ISO/IEC 30111（脆弱性取り扱い手順）の両標準について、作業草案の第 2 版（WD2）に対して各国のエキスパートから寄せられたコメントのうち、特に議論が必要とされた複数のコメントの取り扱いについて検討しました。主に、脆弱性情報の公表猶予期間、AI の能力、サプライチェーン、クラウドに関する事項が議論されました。これらの議論の結果およびコメントを踏まえた変更を作業草案に反映し、再度改版した第 3 版（WD3）を 2026 年 11 月までに作成することになりました。

5.6 脆弱性調整および情報流通に関する国際的な協力体制の構築

JPCERT/CC は、世界各地域で脆弱性調整を担う組織と協力関係を結び、国際的な活動の調整や情報共有などにおいて相互に連携しています。また、FIRST をはじめとする脆弱性に関わる国際的なコミュニティ活動に参加し、連携のための基盤づくりなどを行っています。

第 6 章

フィッシング対策協議会活動

フィッシング対策協議会（本章において、以下「協議会」）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討等を行う会員組織です。JPCERT/CC は、経済産業省からの委託によって、協議会の活動のうち、一般消費者からのフィッシングに関する報告・問い合わせの受け付け、フィッシングサイトに関する注意喚起、一部のワーキンググループの運営等を行っています。

また、協議会は報告を受けたフィッシングサイトについて JPCERT/CC に報告しており、これを受けて JPCERT/CC がインシデント対応支援活動の一環としてフィッシングサイトを停止するための調整等を行っています。

協議会では、経済産業省から委託された活動のほかに、会員組織向けの独自の活動を運営委員会の決定に基づいて行っており、JPCERT/CC は事務局としてこれらの活動の実施についても支援しています。具体的には「[6.2 フィッシング対策協議会の会員組織向け活動](#)」に記載した活動が該当します。

本章では本四半期におけるこれら活動について記載します。

6.1 フィッシング対策協議会事務局の運営

6.1.1 フィッシングに関する報告・問い合わせの受け付け

本四半期分はまだ確定していないものの、フィッシングの報告件数は前四半期に引き続き減少する見通しです。一方で、報告のあったフィッシングサイトの URL のうち、重複を除いた件数（フィッシングサイト数）は必ずしも減少傾向を示していません。

これには、送信ドメイン認証やメールフィルタリングの強化、金融機関における多要素認証やパスキー等の導入、インフラ企業と法執行機関が連携した国際的なサイバー犯罪インフラの無力化活動など、攻撃者を取り巻く環境の変化があると考えられます。また、攻撃手法についても、大量のフィッシングメールを一斉に配信して成功数を稼ぐ手法から、配信規模を抑えながらも、メールの到達率や攻撃の成功率を高めようとする手法へ変化している可能性があります。

こうした動きの一例として、フィッシングメールの件名、文面に不可視の Unicode 文字や RTL 文字（右から左へ読む文字）を埋め込むほか、正規クラウドインフラから送信するなど、メールフィルターを回避して到達率を高めようとする試みが、短期間にブランドを変えて行われていることを確認しています。



図 6.1 不正アプリのインストールへ誘導するフィッシングメールの例

2026 年 9 月には Android 端末向けに不正アプリをインストールさせる手口も見られ（図 6.1）、新たな犯罪インフラ構築をもくろんでいる可能性もあります。このような状況から、報告件数減少のみをもってフィッシング詐欺活動全体が沈静化しつつあるとは判断できず、今後も注意が必要です。

過去 1 年間のフィッシング報告件数の推移を図 6.2 に示します。

本四半期の報告件数の内訳では、Amazon をかたるフィッシングの報告が最も多く、全体の約 28.7% を占めました。次いで、Apple をかたるフィッシングの報告が多く、全体の約 13.3% を占めました。

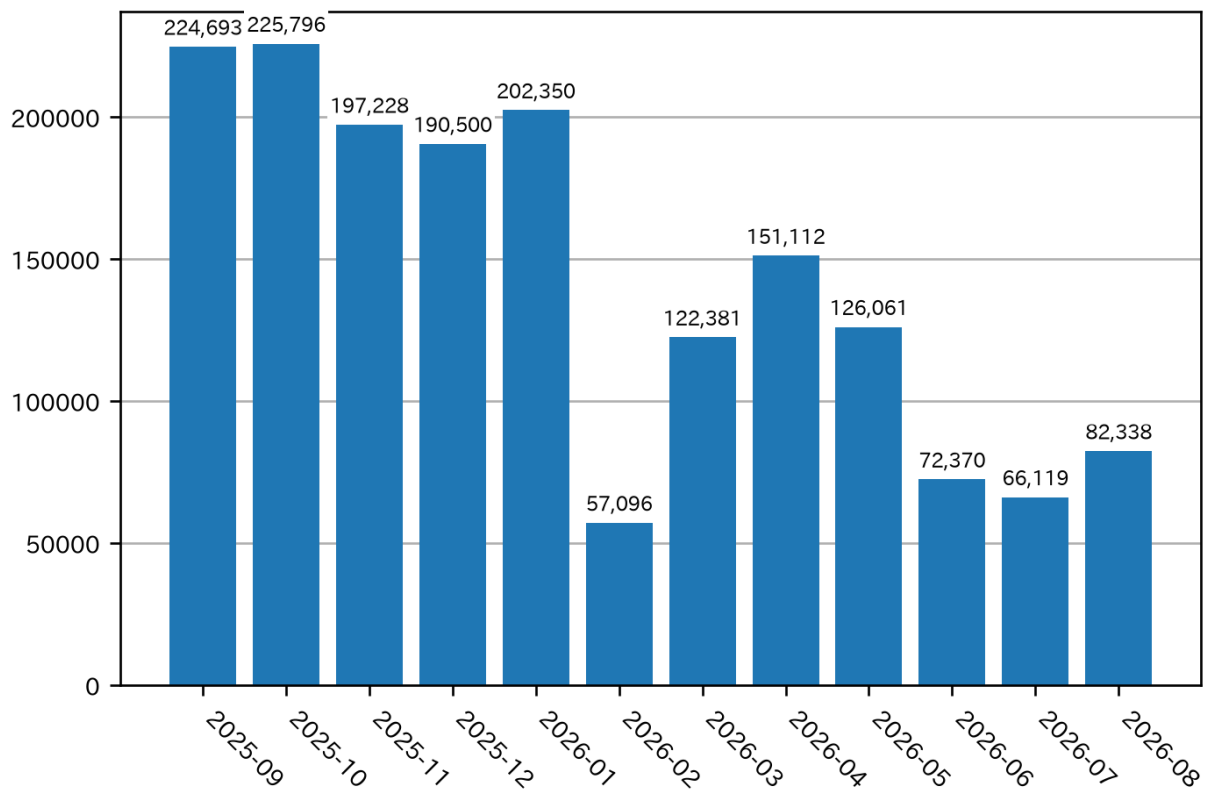


図 6.2 フィッシング報告件数

6.1.2 情報収集／配信

6.1.2.1 定期報告

報告されたフィッシングサイト数や毎月の活動報告等を協議会の Web サイトで公開しました。

- フィッシング対策協議会 Web サイト
<https://www.antiphishing.jp/>
- 2026/06 フィッシング報告状況
<https://www.antiphishing.jp/report/monthly/202606.html>
- 2026/07 フィッシング報告状況
<https://www.antiphishing.jp/report/monthly/202607.html>
- 2026/08 フィッシング報告状況
<https://www.antiphishing.jp/report/monthly/202608.html>

6.1.2.2 フィッシングサイト URL 情報の提供

フィッシング対策ツールバーやアンチウイルスソフトなどを提供している事業者やフィッシングに関する研究を行っている学術機関である協議会の会員等に対し、協議会に報告されたフィッシングサイトの URL を集めたリストを提供しています。これは、フィッシング対策製品の強化や、関連研究の促進を目

的としたものです。本四半期末時点で 51 組織に情報を提供しており、今後も要望に応じて広く提供する予定です。

6.1.2.3 フィッシング対策ガイドライン等の改定作業

「技術・制度検討ワーキンググループ」は、フィッシング対策に関するガイドラインや動向レポートを作成・改訂を行う作業部会で、協議会の会員を中心とする有識者で構成されています。本四半期は、2027 年版のガイドラインおよびレポートの改訂に向けて、次のとおり会合を開催し、最近のフィッシングの傾向、関連技術、法制度の整備状況等について情報共有をしたほか、事業者および一般消費者が講じるべきフィッシング対策等について議論しました。

- 第 1 回技術・制度検討ワーキンググループ
開催日：2026 年 9 月 4 日

6.2 フィッシング対策協議会の会員組織向け活動

運営委員会の決定に基づいて行っている会員組織向けの独自の活動について、JPCERT/CC は事務局として次のとおり支援しました。

6.2.1 運営委員会開催

本四半期においては、協議会の活動の企画・運営方針の決定等を行う運営委員会を次のとおり開催しました。

- 第 140 回運営委員会
開催日：2026 年 7 月 30 日
- 第 141 回運営委員会
開催日：2026 年 9 月 17 日

6.2.2 ワーキンググループ会合等 開催支援

本四半期においては、次の協議会のイベントやワーキンググループ等の会合の開催を支援しました。

- リサーチワーキンググループ会合
開催日：2026 年 7 月～2026 年 9 月 隔週火曜日
- 被害状況共有ワーキンググループ会合
開催日：2026 年 7 月 22 日
- 証明書普及促進ワーキンググループ会合
開催日：2026 年 9 月 3 日

第 7 章

広報活動

JPCERT/CC では事業成果について幅広く広報を行い、成果の普及と周知に努めています。情報の配信は、JPCERT/CC Web サイトや X（旧 Twitter）のほか、Web 媒体、放送媒体、出版媒体などの各種媒体を通じて実施しています。また、セミナーやイベントでの登壇などによる情報発信も行っています。

7.1 講演

本四半期は次のセミナーやイベント等で講演しました。

- IEC TC 65 Plenary Automation Forum
タイトル：Perspective of ICS Cyber Security in Japan
講演者：宮地 利雄（技術顧問）
主催：日本電気計測器工業会
講演日：2026 年 7 月 2 日
- 横浜商工会議所 情報関連産業部会主催 講演会・交流会
タイトル：侵入型ランサムウェアの初動対応
講演者：矢野 雄紀（サイバーセキュリティコーディネーショングループ 脅威分析・インシデント対応チーム マルウェアアナリスト／フォレンジックアナリスト）
主催：横浜商工会議所 情報関連産業部会
講演日：2026 年 7 月 9 日
- FY2026 安全大会
タイトル：建設現場で必要なサイバー攻撃への意識
講演者：尾崎 幸也（サイバーセキュリティコーディネーショングループ 脅威分析・インシデント対応チーム マルウェアアナリスト／フォレンジックアナリスト）
主催：NTT データ
講演日：2026 年 7 月 28 日
- 第 39 回クレジットセプター運営会議
タイトル：生成 AI によってサイバー攻撃の何が変わるのか、変わらないのか
講演者：佐々木 勇人（サイバーセキュリティコーディネーショングループ 担当部門長 兼 政策担

当部長 脅威情報アナリスト)
主催：日本クレジット協会
講演日：2026 年 8 月 31 日

7.2 協力・後援

本四半期は次の行事の開催に協力または後援等を行いました。

- Hardening Designers Conference 2026
主催：Hardening Project 実行委員会
開催日：2026 年 7 月 2 日～2026 年 7 月 4 日
- 日本セキュリティ・マネジメント学会第 39 回全国大会
主催：日本セキュリティ・マネジメント学会
開催日：2026 年 8 月 2 日
- Security Management Conference 2026 夏
主催：SB クリエイティブ
開催日：2026 年 8 月 26 日～2026 年 8 月 27 日

7.3 公開資料

本四半期は次の資料を公開しました。

7.3.1 ソフトウェア等の脆弱性関連情報に関する届出状況

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、経済産業省告示「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）等に基づく脆弱性関連情報流通制度の運用の一端を 2004 年 7 月から担っています。この制度の運用に関連した前四半期の活動実績と、同期間中に公表された脆弱性に関する注目すべき動向をまとめてレポートとして公表しています。

- 2026-07-16
ソフトウェア等の脆弱性関連情報に関する届出状況 [2026 年第 2 四半期 (4 月～6 月)]
https://www.jpcert.or.jp/pr/2026/vulnREPORT_2026q2.pdf

7.3.2 公式ブログ「JPCERT/CC Eyes」

JPCERT コーディネーションセンター公式ブログ「JPCERT/CC Eyes」は、JPCERT/CC が分析・調査した内容、国内外のイベントやカンファレンスの様子などを JPCERT/CC のアナリストの眼を通して、いち早くお届けする読み物です。

本四半期においては次の 5 件の記事を公開しました。

日本語版発行件数：2 件 <https://blogs.jpcert.or.jp/ja/>

- 2026-07-13
APT-C-60 による 2026 年の攻撃
- 2026-07-30
TSUBAME レポート Overflow (2026 年 4～6 月)

英語版発行件数：3 件 <https://blogs.jpcert.or.jp/en/>

- 2026-07-13
Update on Attacks by Threat Group APT-C-60 in 2026
- 2026-07-23
TSUBAME Report Overflow (Jan-Mar 2026)
- 2026-09-18
TSUBAME Report Overflow (Apr-Jun 2026)

付録 A

インシデントの分類

JPCERT/CC では、寄せられた報告に含まれるインシデントを次の定義に従って分類しています。

フィッシングサイト

フィッシングサイトとは、銀行やオークション等のサービス事業者の正規サイトを装い、利用者の ID やパスワード、クレジットカード番号等の情報をだまし取る「フィッシング詐欺」に使用されるサイトを指します。

JPCERT/CC では、以下を**フィッシングサイト**に分類しています。

- 金融機関やクレジットカード会社等のサイトに似せた Web サイト
- フィッシングサイトに誘導するために設置された Web サイト

Web サイト改ざん

Web サイト改ざんとは、攻撃者もしくはマルウェアによって、Web サイトのコンテンツが書き換えられた（管理者が意図したものではないスクリプトの埋め込みを含む）サイトを指します。

JPCERT/CC では、以下を**Web サイト改ざん**に分類しています。

- 攻撃者やマルウェア等により悪意のあるスクリプトや iframe 等が埋め込まれたサイト
- SQL インジェクション攻撃により情報が改ざんされたサイト

マルウェアサイト

マルウェアサイトとは、閲覧することで PC がマルウェアに感染してしまう攻撃用サイトや、攻撃に使用するマルウェアを公開しているサイトを指します。

JPCERT/CC では、以下を**マルウェアサイト**に分類しています。

- 閲覧者の PC をマルウェアに感染させようとするサイト
- 攻撃者によりマルウェアが公開されているサイト

スキャン

スキャンとは、サーバーや PC 等の攻撃対象となるシステムの存在確認やシステムに不正に侵入するための弱点（セキュリティホール等）探索を行うために、攻撃者によって行われるアクセス（システムへの影響がないもの）を指します。また、マルウェア等による感染活動も含まれます。

JPCERT/CC では、以下を**スキャン**と分類しています。

- 弱点探索（プログラムのバージョンやサービスの稼働状況の確認等）
- 侵入行為の試み（未遂に終わったもの）
- マルウェア（ウイルス、ボット、ワーム等）による感染の試み（未遂に終わったもの）
- ssh、ftp、telnet 等に対するブルートフォース攻撃（未遂に終わったもの）

DoS/DDoS

DoS/DDoS とは、ネットワーク上に配置されたサーバーや PC、ネットワークを構成する機器や回線等のネットワークリソースに対して、サービスを提供できないようにする攻撃を指します。

JPCERT/CC では、以下を **DoS/DDoS** と分類しています。

- 大量の通信等により、ネットワークリソースを枯渇させる攻撃
- 大量のアクセスによるサーバープログラムの応答の低下、もしくは停止
- 大量のメール（エラーメール、SPAM メール等）を受信させることによるサービス妨害

ランサム攻撃

ランサム攻撃とは、ファイルの暗号化・削除、情報の持ち出し、身代金要求などを伴う、またはこれらにつながる攻撃を指します。

JPCERT/CC では、以下を**ランサム攻撃**と分類しています。

- ランサムウェア攻撃：ランサムウェアを使用し、ファイルの暗号化などを行う攻撃
- 侵入型ランサムウェア攻撃：企業や組織の内部ネットワークに攻撃者が侵入した後、情報窃取やランサムウェアなどを用いたファイルの暗号化などを行う攻撃
- 身代金要求型攻撃：ファイルの暗号化・削除や情報窃取などを行い、その復旧や情報の非公開などと引き換えに身代金を要求する攻撃

制御システム関連インシデント

制御システム関連インシデントとは、制御システムや各種プラントが関連するインシデントを指します。

JPCERT/CC では、以下を**制御システム関連インシデント**と分類しています。

- インターネット経由で攻撃が可能な制御システム
- 制御システムを対象としたマルウェアが通信を行うサーバー
- 制御システムに動作異常等を発生させる攻撃

標的型攻撃

標的型攻撃とは、特定の組織、企業、業種などを標的として、マルウェア感染や情報の窃取などを試みる攻撃を指します。

JPCERT/CC では、以下を**標的型攻撃**と分類しています。

- 特定の組織に送付された、マルウェアが添付されたなりすましメール
- 閲覧する組織が限定的である Web サイトの改ざん
- 閲覧する組織が限定的である Web サイトになりすまし、マルウェアに感染させようとするサイト
- 特定の組織を標的としたマルウェアが通信を行うサーバー

その他

その他とは、上記以外のインシデントを指します。

JPCERT/CC が**その他**に分類しているものの例を次に掲げます。

- 脆弱性等を突いたシステムへの不正侵入
- ssh、ftp、telnet 等に対するブルートフォース攻撃の成功による不正侵入
- キーロガー機能を持つマルウェアによる情報の窃取
- マルウェア（ウイルス、ボット、ワーム等）の感染

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) まで確認のご連絡をお願いします。

本文書に記載の社名、製品名は各社の商標または登録商標です。

最新情報については JPCERT/CC の Web サイトをご参照ください。

- JPCERT コーディネーションセンター (JPCERT/CC) : <https://www.jpcert.or.jp/>
- インシデント情報の提供および対応依頼 : info@jpcert.or.jp, <https://www.jpcert.or.jp/form/>
- 脆弱性情報ハンドリングに関するお問い合わせ : vultures@jpcert.or.jp
- 制御システムセキュリティに関するお問い合わせ : dc-info@jpcert.or.jp
- セキュアコーディングセミナーのお問い合わせ : secure-coding@jpcert.or.jp
- 公開資料の引用、講演依頼、その他のお問い合わせ : pr@jpcert.or.jp
- PGP 公開鍵について : <https://www.jpcert.or.jp/jpcert-pgp.html>

JPCERT/CC 四半期レポート [2026 年 7 月 1 日～2026 年 9 月 30 日]

- 発行履歴
 - 2026 年 10 月 22 日 初版
- 発行者
 - 一般社団法人 JPCERT コーディネーションセンター
 - 〒103-0023
 - 東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
 - TEL 03-6271-8901 FAX 03-6271-8908
 - URL <https://www.jpcert.or.jp/>